GFI Product Manual

VIPRE® Antivirus

User Guide

GFI®

Document Version: VAV-UG-EN-5.0

Last updated: 10/25/2011

Table of Contents

1 Introduction

Welcome! VIPRE® Antivirus 2012 offers PC users security against more complex and malicious threats with its powerful anti-malware protection, while eliminating the performance and resource problems of many older, traditional antivirus products. The solution combines antivirus, anti-spyware, anti-rootkit and other technologies into a seamless, tightly-integrated product.

VIPRE (Virus Intrusion Protection Remediation Engine) is uniquely designed to reduce computer frustration with its low system resource usage, faster boot times, few popups, and a broad-range of detection and remediation of viruses, trojans, worms, and spyware.

There are three ways to get information about VIPRE:

The **Quick Start Guide** only covers the basic steps needed to get VIPRE up and running—protecting your computer from viruses, malware, and other unwanted applications right away.

The **Help** is your primary resource for answers to questions you may have while using VIPRE. The Help contains overviews and procedural information about the tasks you can perform in the application, as well as descriptions of each screen and dialog box in the application with detailed information about each field they contain. Whenever you want to know about a screen or dialog box that you are in, you can press F1 on your keyboard or click the **Help button** ? Help. The applicable help topic will display for that screen.

This **User Guide** contains the same information as the Help structured in a way that is to be used as a reference manual.

System Requirements

Your computer must meet the following system requirements in order to run the application effectively:

> **Note:** This product should not be installed on any type of storage media that may be inaccessible at times. This includes network drives, removable drives, hot-swappable drives, USB drives, and FireWire (IEEE 1394) drives that may be disconnected.

- Supported Operating Systems:
  - Windows XP SP2+ (32- & 64-bit)
  - Windows 2003 Server SP1+ (32- & 64-bit)
  - Windows Vista, Vista SP1+ (32- & 64-bit)
  - Windows 7 (32- & 64-bit)
  - Windows Server 2008+ (32- & 64-bit)

  > **Note:** Installation is not supported on Windows 95, 98, ME, NT 4, Win 2000, XP with SP1 or older, Macintosh or Linux computers.

- 1 GHZ Computer with 512 MB of RAM (memory) and 300 MB of available free space on your hard drive.
- Miscellaneous:
  - Microsoft Internet Explorer 6.0 or higher
  - Internet access for definitions updates (Broadband recommended)
  - 2x CDROM if you are having the CD shipped to you (not necessary for online download)
- Supported Email Clients (applies to Email Protection):
  - Outlook 2000+
  - Outlook Express 5.0+
  - Windows Mail on Vista
  - SMTP/POP3 (Thunderbird, IncrediMail, Eudora, etc.)

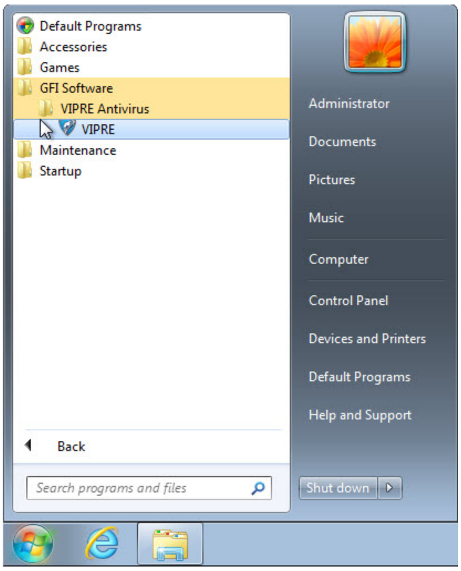
> **Note**: SSL and TLS are supported in Microsoft Outlook and Microsoft Outlook Express only.

Starting VIPRE Antivirus

You can start VIPRE by any of the following ways:

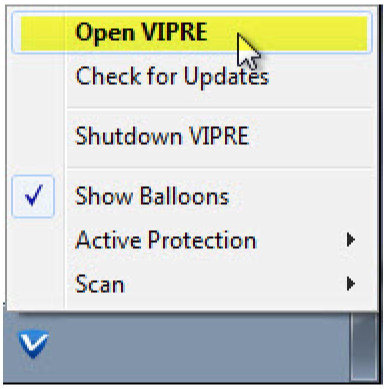
- Double-click the VIPRE icon shortcut (pictured below) on your desktop.

- Click **Start** and then select **All Programs>GFI Software>VIPRE Antivirus>VIPRE Antivirus.**



Screenshot 1: Starting VIPRE Antivirus from the Windows Start menu

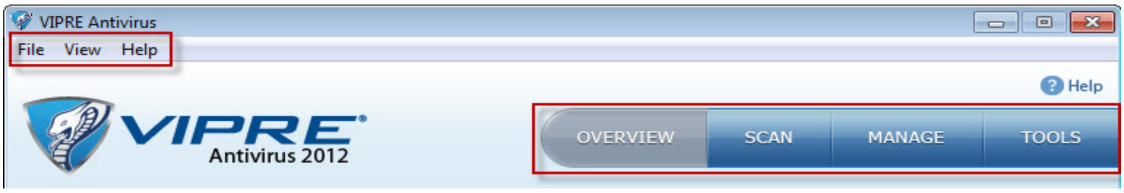
- Right-click on the system tray icon in the lower-right corner of your screen.



Screenshot 2: Starting VIPRE Antivirus from the system tray

Touring the VIPRE Interface

The VIPRE interface uses tabs to display screens from which all work is completed. In addition to the tabs there are also links on the Overview page that open the same pages as the tabs.



Screenshot 3: VIPRE Antivirus top navigation

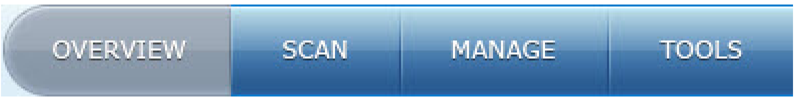
Toolbar Menu

The standard toolbar menu offers one way to access functions within VIPRE. Options include:

- **File**: Allows you to open the Settings dialog box where you can configure all of the detailed settings, or Exit VIPRE.
- **View**: Allows you to go directly to whichever screen you need to. (See list under Tabs below for all screens.)
- **Help**: Allows you to open the Help system, send a file to GFI Software for analysis, register VIPRE, or view the About VIPRE dialog box.

> **Note:** Clicking the **Help** icon in the upper-right corner of the screens displays the help topic for the screen in which you are currently working.

Tabs



Screenshot 4: VIPRE Antivirus tabs

The tabs contain the main functions of the system, with some tabs containing sub-areas that link you to other screens. The breakdown is as follows:

- **Overview**: use this screen to get a quick status look at VIPRE and to quickly access the application's main functions.
- **Scan**: go here to scan your computer.
- **Manage**: go here to work with the results of scans and to schedule automatic scans.
  - **History**: allows you to work with history events, including scan, AP, email, and system events.
  - **Quarantine**: allows you to work with quarantined items.
  - **Always Allowed**: allows you to work with always allowed items.
  - **Schedule Scans**: allows you to schedule scans on your computer to occur automatically.
- **Tools**: go here to access areas of your computer that you don't normally use or see.
  - **Secure File Eraser**: allows you to add an "Erase Files" option to your Window's Explorer menu to erase files from your computer permanently.
  - **History Cleaner**: allows you to remove browsing and search histories from specific applications.
  - **PC Explorer**: allows you to view normally hidden settings of files, applications, and websites based on eight different criteria within your computer, and add programs to your Always Allowed list.

Working with the System Tray Icons

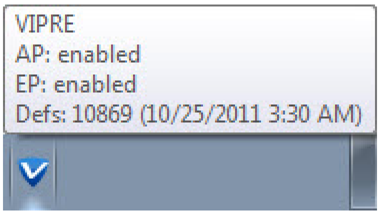
VIPRE uses icons in your system tray with different colors signifying the following:

- **Green** indicates that an active scan is running.
- **Red** indicates that the service is not running and that an error occurred.

- **Gray** indicates that either the firewall and/or Active Protection (AP) are disabled.
- **Blue** indicates that VIPRE is idle and that AP and Email AV Protection are both enabled, actively protecting your computer.
- **Yellow** is the Warning icon alerting you to events, such as the completion of a scan, an update is ready to be installed, or errors. Double-click to open the newest item in the System history.

> **Note:** If you get any errors while running VIPRE, please call GFI Software's Technical Support.

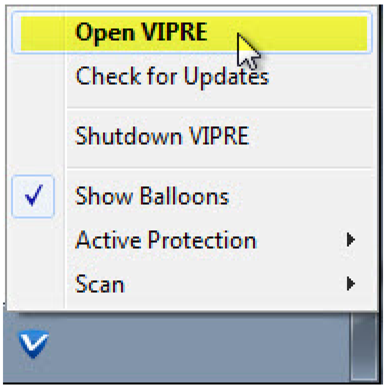
You can hover your mouse arrow over the icons to display hover text displaying the status of VIPRE. VIPRE will also display messages notifying you of the status of scans and updates, as well as the most recent Definitions version and when it was downloaded.



VIPRE
AP: enabled
EP: enabled
Defs: 10869 (10/25/2011 3:30 AM)

Screenshot 5: System tray status balloon

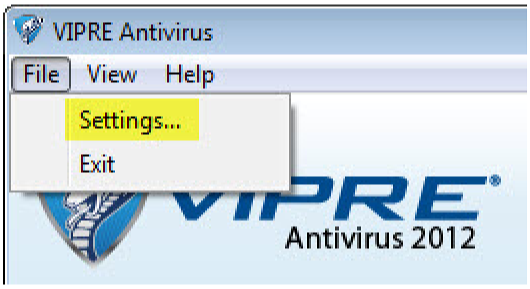
You can also right-click on the primary icon to open/shutdown VIPRE, check for updates, enable/disable Active Protection, run/abort/pause/resume a scan, as well as select to show/hide the balloon notifications.



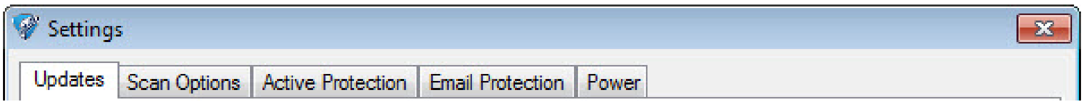
Screenshot 6: System tray right-click options

2 Configuring Settings

Configuring all of VIPRE's settings can be done from one location - the **Settings** dialog box (**File>Settings**).



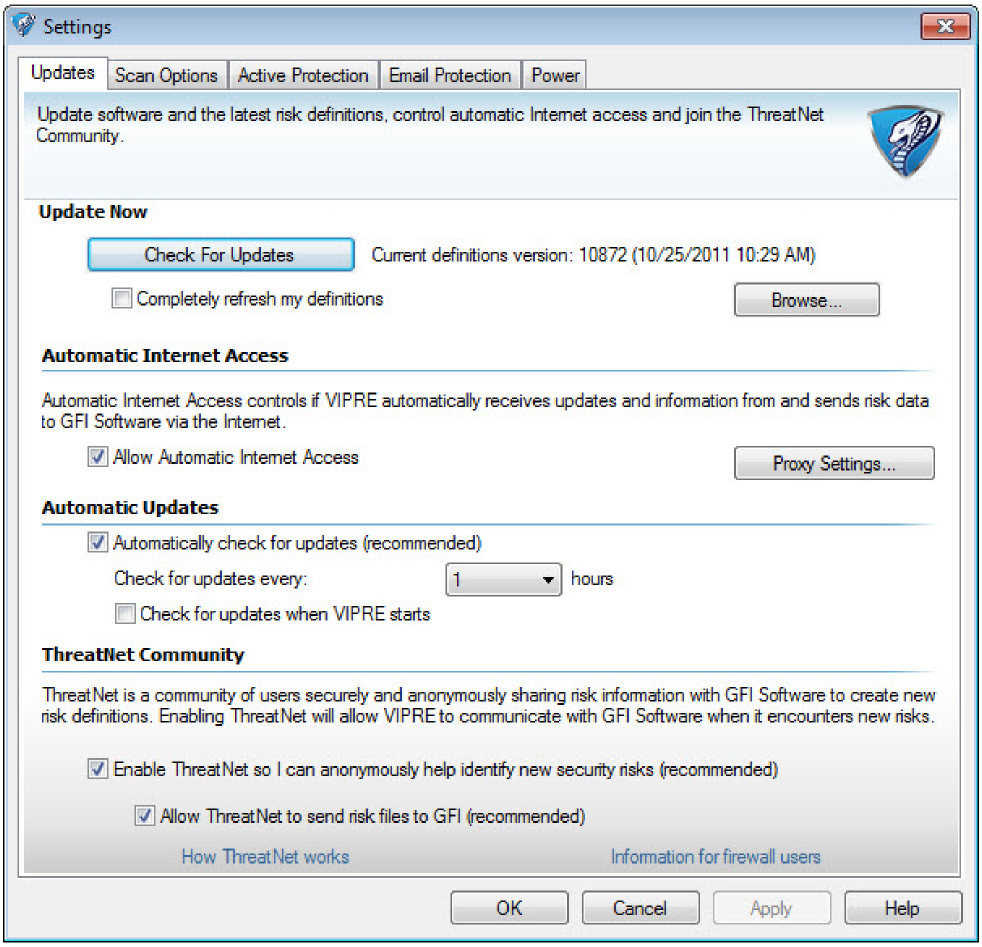
Screenshot 7: File > Settings menu



Screenshot 8: Settings dialog box tabs

Updating VIPRE

VIPRE uses continuously updated definitions to protect you from all sorts of malware. It's important to keep VIPRE updated regularly.



Settings

Updates | Scan Options | Active Protection | Email Protection | Power

Update software and the latest risk definitions, control automatic Internet access and join the ThreatNet Community.

Update Now

Check For Updates   Current definitions version: 10872 (10/25/2011 10:29 AM)

☐ Completely refresh my definitions   Browse...

Automatic Internet Access

Automatic Internet Access controls if VIPRE automatically receives updates and information from and sends risk data to GFI Software via the Internet.

☑ Allow Automatic Internet Access   Proxy Settings...

Automatic Updates

☑ Automatically check for updates (recommended)

Check for updates every: 1 hours

☐ Check for updates when VIPRE starts

ThreatNet Community

ThreatNet is a community of users securely and anonymously sharing risk information with GFI Software to create new risk definitions. Enabling ThreatNet will allow VIPRE to communicate with GFI Software when it encounters new risks.

☑ Enable ThreatNet so I can anonymously help identify new security risks (recommended)

☑ Allow ThreatNet to send risk files to GFI (recommended)

How ThreatNet works   Information for firewall users

OK | Cancel | Apply | Help

Screenshot 9: Settings > Updates screen

To manually get updates:

From the **Overview** screen, click **Update Now**. VIPRE checks for updates and, if there are any updates available, downloads and applies them. The VIPRE Update Progress dialog box displays the status of the update.

Completely refresh my definitions: Instead of getting incremental updates, VIPRE will reinstall the entire security risk database. This option is rarely necessary. If necessary (usually under the assistance of Technical Support), select this option before clicking **Check for Updates**. This is a larger file size than the updates and will take longer to download.

To set automatic updates:

Automatic Updates will automatically update both definitions and software, if available.

1. From the **Updates** area on the **Overview** screen, click **Settings**. The Updates tab in the Settings dialog box displays.
2. Ensure that the **Allow Automatic Internet Access** checkbox is selected. If deselected, VIPRE will not be able to connect to the Internet to get updates.
3. Optionally, if you connect via a proxy, click Proxy Settings to configure the proxy.
4. Select the **Automatically check for updates** checkbox.
5. Click the **hours** drop-down arrow and select how frequently you want VIPRE to check for updates.

   Note: It is recommended to set this to 1 hour, which is the default. A one hour setting help ensures that the updates are small and fast.

6. Optionally, select **Check for updates when VIPRE starts.**

   When selected and when the VIPRE service starts (i.e. at boot-time and manual start), VIPRE will immediately check for definitions updates.

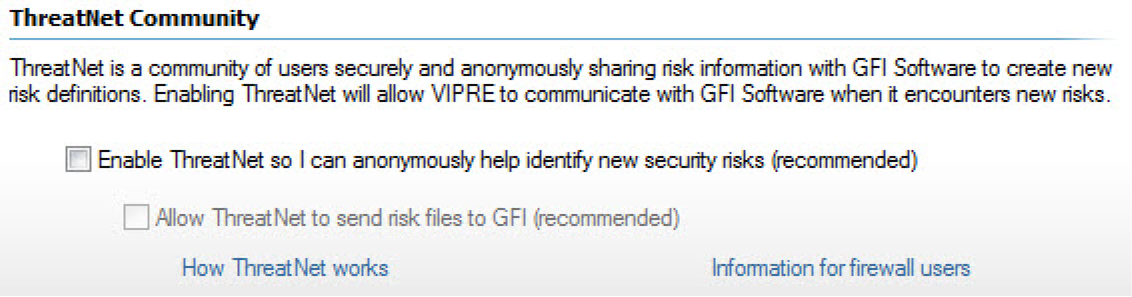
7. Click **OK** to accept changes and close the dialog box.

During the scheduled update, VIPRE will apply definition updates automatically as they become available. If a software update is available, you will be prompted to install the software update.

Enabling ThreatNet

ThreatNet™ helps GFI Software to continually make VIPRE Antivirus better at protecting your computer.

Note: Go to http://www.gfi.com/pages/privacy.htm to view GFI Software's privacy policy.



ThreatNet Community

ThreatNet is a community of users securely and anonymously sharing risk information with GFI Software to create new risk definitions. Enabling ThreatNet will allow VIPRE to communicate with GFI Software when it encounters new risks.

☐ Enable ThreatNet so I can anonymously help identify new security risks (recommended)

☐ Allow ThreatNet to send risk files to GFI (recommended)

Screenshot 10: ThreatNet Community area on the Settings > Updates screen

To enable ThreatNet:

1. From the **Updates** area on the **Overview** screen, click **Settings.** The Updates tab in the Settings dialog box displays.
2. In the **ThreatNet Community** area, select the following:
   - **Enable ThreatNet so I can anonymously help identify new security risks (recommended):** Select to enable ThreatNet and join a community of users sharing information with GFI Software about potential risks.
   - **Allow ThreatNet to send risk files to GFI (recommended):** With this option selected and when VIPRE discovers an unknown potential risk, this file will be automatically sent to GFI Software for analysis. With this option not selected, risk files will not be sent.
3. Click **OK** to save settings.

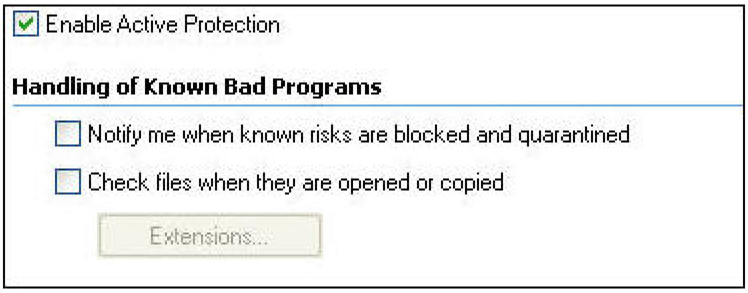
Configuring Active Protection

Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your computer system.

> Warning: When using Active Protection, ensure that there is no other real-time protection software running. If there is another real-time software running, the two programs running together may cause a noticeable decrease in system performance.

To set and configure Active Protection:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Active Protection** tab.
3. To enable AP, select the **Enable Active Protection** checkbox.
   -or-
   To disable AP, unselect the **Enable Active Protection** checkbox. Known risks will not be stopped in real-time; instead, they will be detected during scans. Skip to step 5.



☑ Enable Active Protection

Handling of Known Bad Programs

☐ Notify me when known risks are blocked and quarantined

☐ Check files when they are opened or copied

Screenshot 11: Active Protection screen options

4. In the **Handling of Known Bad Programs** area, select or unselect the following:
   - **Notify me when known risks are blocked and quarantined:** select this checkbox to see VIPRE working as it detects, blocks, and quarantines known risks. You can work with quarantined items at a later time. Unselect this checkbox to not be bothered by notifications; known risks will continue to be automatically quarantined. You can view AP history periodically to view a log of what AP has

detected.

- **Check files when they are opened or copied**: Select this checkbox for AP to automatically scan a file when it is accessed. Scanned files include EXE, INI, HLP, BAT, and others.
- **Extensions**: (advanced) Once the **Check files when they are opened or copied** option is selected, this button is enabled. Click to open the AP File Extensions dialog box, which allows you to set file extensions that will be checked by AP.

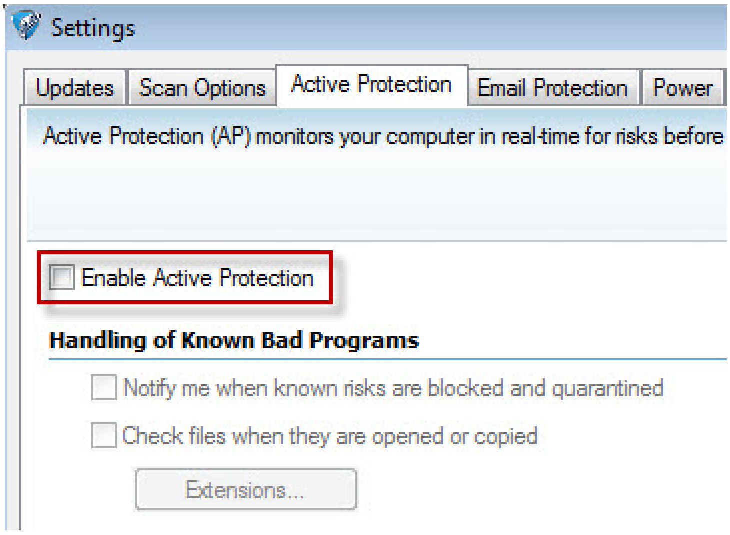
5. Click **OK**. Your AP settings are now applied.

Disabling Active Protection

You can turn off Active Protection (AP) from the settings dialog box or from the system tray. Turning AP off from the dialog box requires you to manually turn it back on yourself when you want it on again. Turning AP off from the system tray allows you to turn it off for a designated period.

To disable Active Protection from the Settings:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Active Protection** tab.
3. To disable AP, unselect the **Enable Active Protection** checkbox. All of the fields in the screen will be grayed out.



Active Protection (AP) monitors your computer in real-time for risks before

□ Enable Active Protection

Handling of Known Bad Programs

□ Notify me when known risks are blocked and quarantined

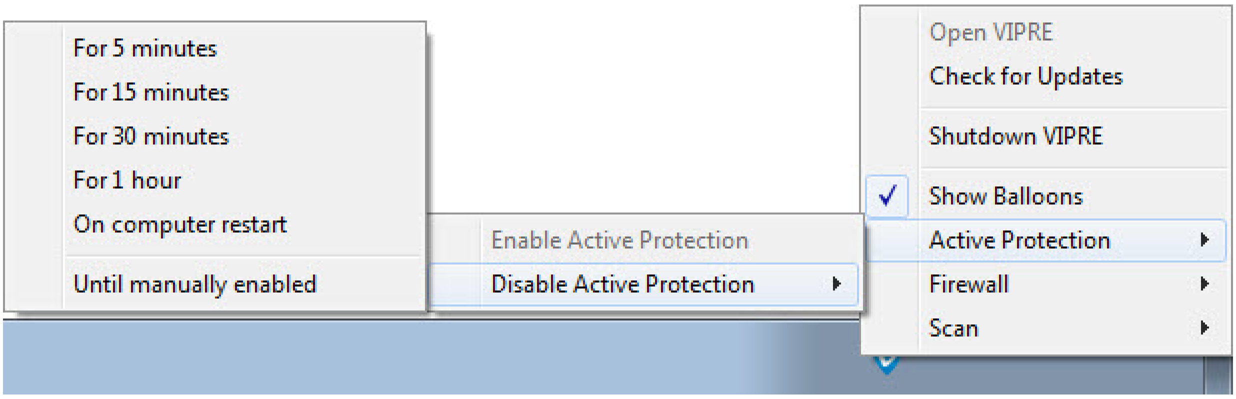
□ Check files when they are opened or copied

Screenshot 12: Disabling Active Protection

4. Click **OK**. AP is now disabled.

To disable Active Protection from the system tray:

1. Right-click on the VIPRE icon in the system tray and select **Active Protection**, and then **Disable Active Protection**.



Screenshot 13: Active Protection options in system tray

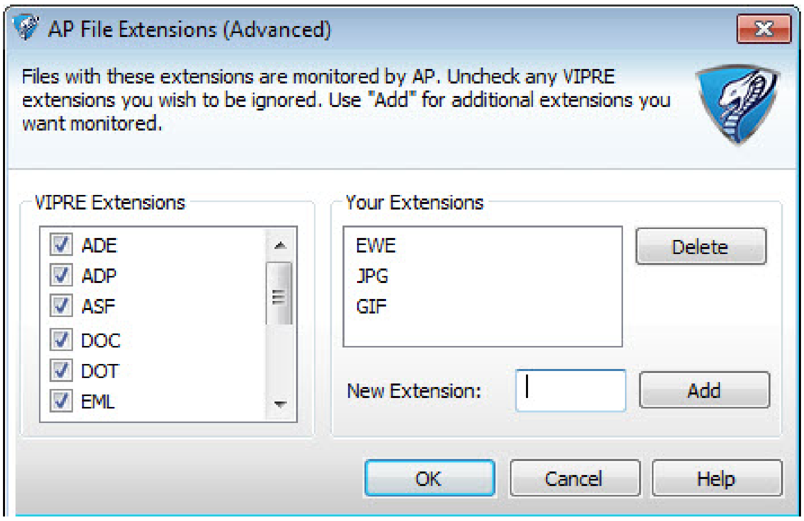
2. Choose from any of the following options below for a set period of time, after which AP will be turned back on:
   - For 5 minutes
   - For 15 minutes
   - For 30 minutes
   - For 1 hour
   - On computer restart
   - Until manually enabled

Note: At any time during the selected time above, you can turn AP back on.

AP File Extensions (Advanced) Dialog Box

The **AP File Extensions** dialog box is an advanced tool allowing you to set file extensions that will be checked by AP. In addition to everything else that AP monitors, AP will monitor files with these extensions when they are opened, closed, or dragged/dropped onto any of your computer's drives.

This dialog box is accessible from **File>Settings>Active Protection** tab>click **Enable Active Protection**>click **Check files when they are opened or copied**>click **Extensions...** button.



AP File Extensions (Advanced)

Files with these extensions are monitored by AP. Uncheck any VIPRE extensions you wish to be ignored. Use "Add" for additional extensions you want monitored.

Screenshot 14: Active Protection File Extensions

This dialog box contains the following items:

- **VIPRE Extensions**: Displays the list of extensions that VIPRE will automatically check on access. Select or deselect any of the listed extensions and click **OK**.
- **Your Extensions**: Displays the list of user-added extensions that VIPRE will automatically check on access.
- **New Extension**: Enter a file extension limited to 10 characters and NO periods. It is not case-sensitive. The extension will then appear in the Your Extensions list. Wildcards are not supported.
- **Delete**: Select an extension from the **Your Extensions** list area and click **Delete**.
- **Add**: After entering the file extension, click **Add**. The extension will be displayed in Your Extensions list area.
- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.

About Email Protection

Note: SSL and TLS are supported in Microsoft Outlook and Microsoft Outlook Express only.

What is Email Protection and how does it work?

Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything.

What email programs/clients are supported by VIPRE's Email Protection?

VIPRE supports the following email programs: MS Outlook 2000+, Outlook Express 6.0+, and Windows Mail. Any POP3/SMTP client is also supported. When using a POP3/SMTP client, you must verify that the port settings of your email provider match VIPRE's port settings. Please refer to your email provider's documentation for correct port settings.

VIPRE does not support the Internet Message Access Protocol (IMAP) for non-Microsoft email programs or encrypted email traffic.

If you use an Internet browser such as Internet Explorer (IE) or Firefox to access email, VIPRE's Email Protection does not apply; in this case, your computer would be protected through Active Protection.

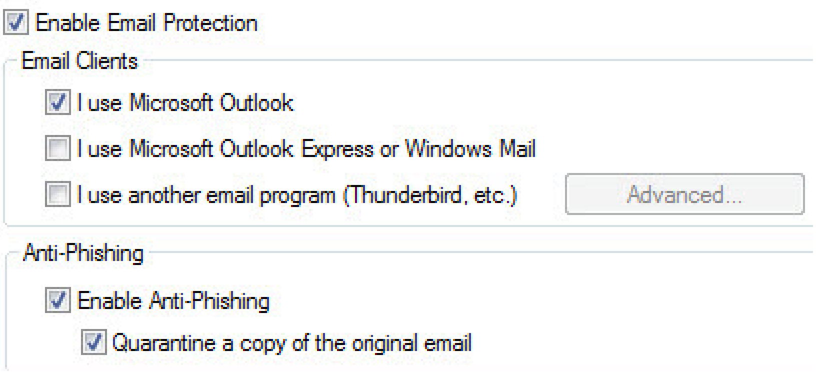
How can I see what VIPRE's Email Protection finds?

VIPRE maintains a history of all of its detections in the View Email History screen (**MANAGE** tab>**View history** link>**EMAIL** tab). You can also view the items put in quarantine from the Quarantine screen (**MANAGE>View quarantine** link).

Configuring Email Protection

Note: If you use a POP3/SMTP client, ensure your port settings are correct.

Note: SSL and TLS are supported in Microsoft Outlook and Microsoft Outlook Express only.



☑ Enable Email Protection

Email Clients

☑ I use Microsoft Outlook

□ I use Microsoft Outlook Express or Windows Mail

□ I use another email program (Thunderbird, etc.)

Anti-Phishing

☑ Enable Anti-Phishing

☑ Quarantine a copy of the original email

Screenshot 15: Email Protection settings

To configure Email Protection:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Email Protection** tab.
3. Select the **Enable email protection** checkbox for VIPRE to scan all incoming and outgoing emails.
4. Select the email program(s) that you use:

    - **I use Microsoft Outlook**: Select this option if you use this program to check your email.
    - **I use Microsoft Outlook Express or Windows Mail:** Select this option if you use either of these programs to check your email.
    - **I use another email program (Thunderbird, etc.)**: Select this option if you use a program other than a Microsoft program to check your email. Once selected, the Advanced button becomes enabled.

5. If you only selected a Microsoft option, skip to the next step.
   -or-
   If you selected "I use another email program" as one of your options AND your email program requires you to change your email port settings from the default, configure the email port settings:

    - Click **Advanced**. The Advanced Email Port Settings dialog box displays.
    - Enter Email Port Settings:

        - **Inbound (POP3)**: Set this number to match both the POP3 number that your email provider uses AND what is set for your email application, as applicable. The default POP3 port is 110.
        - **Outbound (SMTP)**: Set this number to match both the SMTP number that your email provider uses AND what is set for your email application, as applicable. The default SMTP port is 25.

    - Click **OK**. Your port settings are saved and you are returned to the Settings dialog box.

6. Configure anti-phishing:

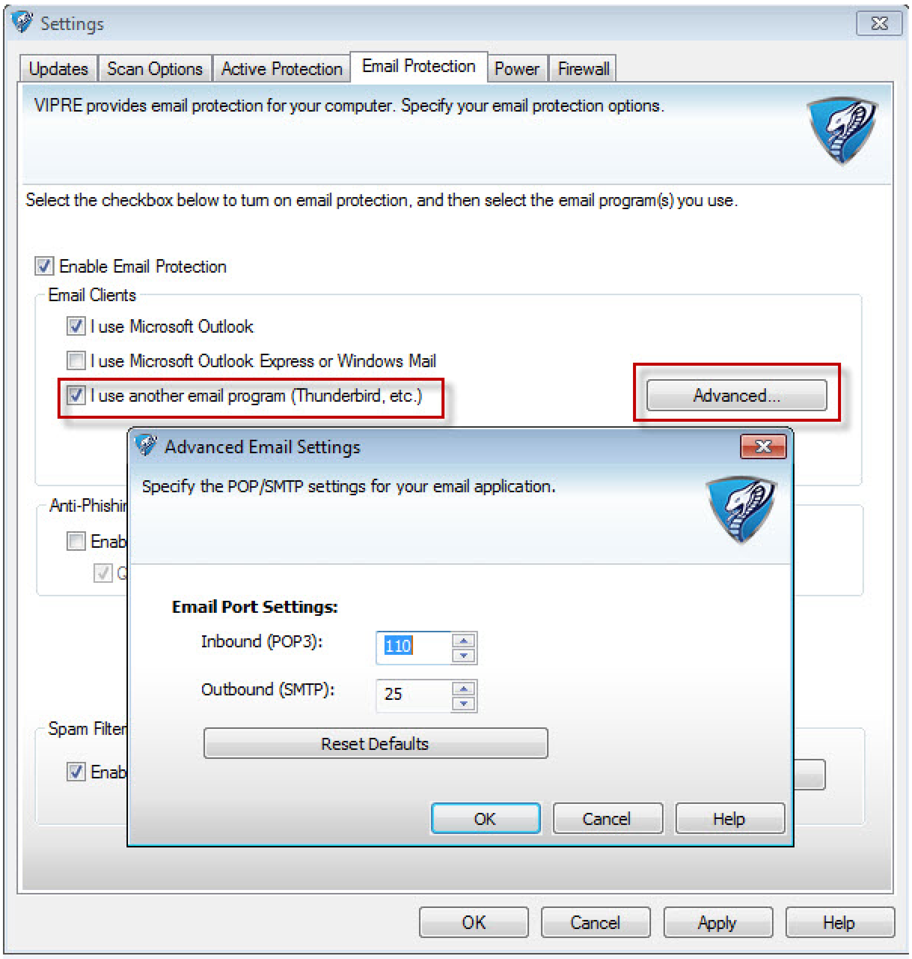
    - **Enable Anti-Phishing**: Select to enable anti-phishing. When enabled and you receive a phishing email, VIPRE strips the known bad URL link from the email, protecting you from the phishing scam.

- **Quarantine a copy of the original email**: Select to save an original copy of the email to the quarantine folder.

7. Click **OK**. Your Email Protection settings are saved.

Configuring Advanced Email Port Settings

If you are using Microsoft Outlook 2000+, Microsoft Outlook Express 6.0+, or Windows Mail on Vista, you will most likely NOT need to change your email port settings. If, however, your Email Provider requires you to change your Email port settings, you will need to enter those same settings here. Contact your email provider or look in your email application for the correct email port settings.



VIPRE provides email protection for your computer. Specify your email protection options.

Select the checkbox below to turn on email protection, and then select the email program(s) you use.

☑ Enable Email Protection

Email Clients

☑ I use Microsoft Outlook

□ I use Microsoft Outlook Express or Windows Mail

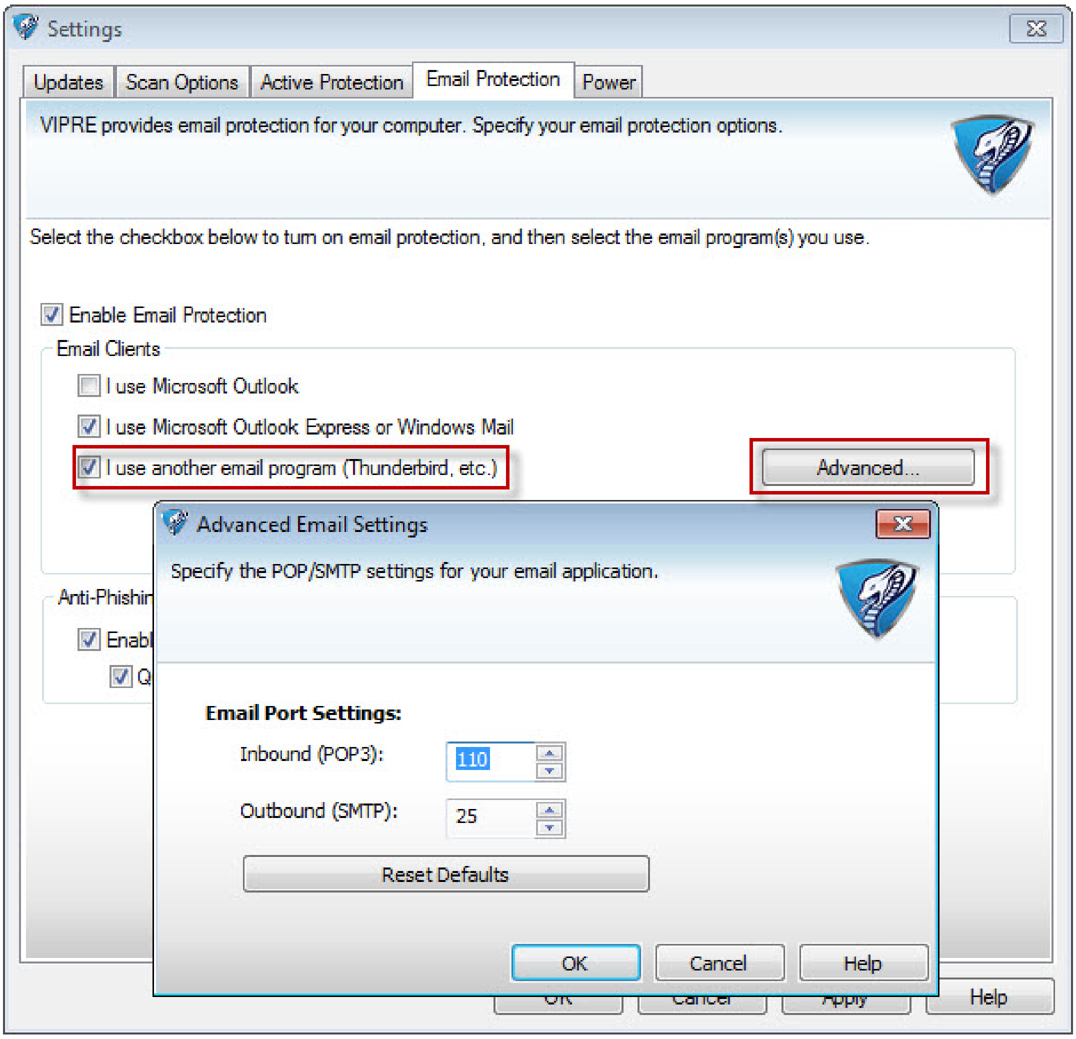
☑ I use another email program (Thunderbird, etc.)

Specify the POP/SMTP settings for your email application.

Email Port Settings:

Inbound (POP3): 110

Outbound (SMTP): 25



Settings

Updates | Scan Options | Active Protection | Email Protection | Power

VIPRE provides email protection for your computer. Specify your email protection options.

Select the checkbox below to turn on email protection, and then select the email program(s) you use.

☑ Enable Email Protection

Email Clients

☐ I use Microsoft Outlook

☑ I use Microsoft Outlook Express or Windows Mail

☑ I use another email program (Thunderbird, etc.)

Advanced...

Anti-Phishin

☑ Enabl

☑ Q

Advanced Email Settings

Specify the POP/SMTP settings for your email application.

Email Port Settings:

Inbound (POP3): 110

Outbound (SMTP): 25

Reset Defaults

OK | Cancel | Help

OK | Cancel | Apply | Help

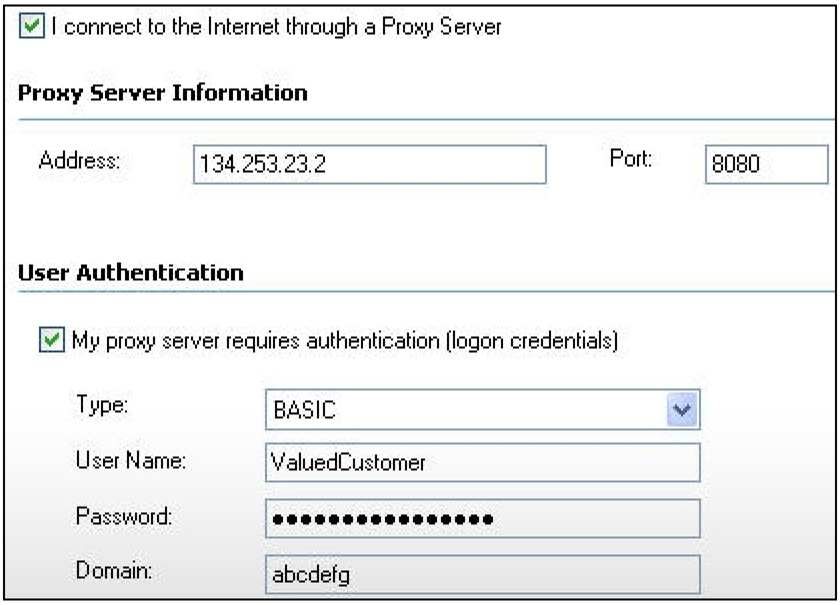
Screenshot 16: Advanced email port settings

To configure email port settings in VIPRE:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Email Protection** tab.
3. Select the **Enable email protection** checkbox for VIPRE to scan all incoming and outgoing emails.
4. Click **Advanced**. The Advanced Email Port Settings dialog box displays.
5. Enter Email Port Settings:
   - **Inbound (POP3):** Set this number to match both the POP3 number that your email provider uses AND what is set for your email application, as applicable. The default POP3 port is 110.
   - **Outbound (SMTP):** Set this number to match both the SMTP number that your email provider uses AND what is set for your email application, as applicable. The default SMTP port is 25.
6. Click **OK**. Your port settings are saved and you are returned to the Settings dialog box.
7. Click **OK**. Your Email Protection settings are saved.

Setting up a Proxy Server

If you use a proxy to connect to the Internet, enter the information here. For most home users, this procedure won't apply because a Proxy is generally used in corporate networks. If you think you may need to use a proxy and do not know how to acquire the necessary information, you can consult your Internet Service Provider (ISP) or network administrator to obtain proxy information.



☑ I connect to the Internet through a Proxy Server

Proxy Server Information

Address: 134.253.23.2

Port: 8080

User Authentication

☑ My proxy server requires authentication (logon credentials)

Type: BASIC

User Name: ValuedCustomer

Password: ●●●●●●●●●●●●●●●●

Domain: abcdefg

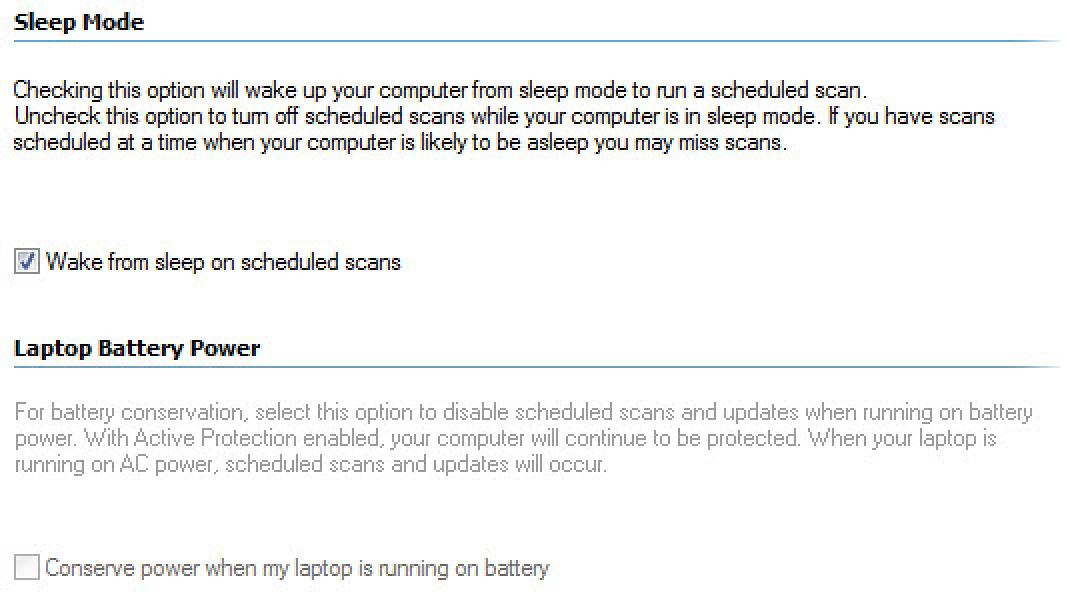
Screenshot 17: Proxy Settings

To set up a proxy server:

1. From the **File** menu, select **Settings**. The Settings dialog box displays the default **Updates** tab.
2. Click **Proxy Settings**. The Proxy Settings dialog box.
3. Select the **I connect to the Internet through a Proxy Server** checkbox.
4. Enter the **Proxy Server Information**:
   - **Address**: Enter the IP Address (i.e. 10.3.120.3) of a server that you are connected or the server name (i.e. OurServer).
   - **Port**: Enter the port number (i.e. 8080) of the server that is used to connect to the Internet.
5. If the server to which you are connecting for Internet access requires login credentials, select the **My proxy server requires authentication** checkbox.
6. Enter the **User Authentication** information provided by your Internet Service Provider or Network Administrator.
7. Click **OK**. Your proxy settings are enabled, allowing VIPRE to establish an Internet connection.

Configuring Power Save Options

Set how VIPRE operates when your computer runs under certain power conditions in order to conserve power. Also, set how VIPRE will work on laptops and on all computers when in sleep mode.



Sleep Mode

Checking this option will wake up your computer from sleep mode to run a scheduled scan.
Uncheck this option to turn off scheduled scans while your computer is in sleep mode. If you have scans scheduled at a time when your computer is likely to be asleep you may miss scans.

☑ Wake from sleep on scheduled scans

Laptop Battery Power

For battery conservation, select this option to disable scheduled scans and updates when running on battery power. With Active Protection enabled, your computer will continue to be protected. When your laptop is running on AC power, scheduled scans and updates will occur.

□ Conserve power when my laptop is running on battery

Screenshot 18: Power save options

To set VIPRE's behavior when your computer is asleep:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. From the **Settings** dialog box, click the **Power** tab.
3. To wake your computer when it is in sleep mode to run a scheduled scan, select **Wake from sleep on scheduled scans**. This is the recommended setting.

   -or-

   To NOT wake your computer when it is in sleep mode to run a scheduled scan, unselect **Wake from sleep on scheduled scans**.

   > **Warning:** When you use Windows sleep mode and unselect this option, your computer may be at risk of missing important system scans, especially during periods of inactivity. To ensure that your computer is protected, you can run a scan manually or schedule a scan at a time that your computer is not asleep.

4. Click **OK** to accept changes and close the dialog box.

To set VIPRE to conserve your laptop's battery:

> **Note:** This does not apply to desktop PCs. This only applies to laptop computers.

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. From the **Settings** dialog box, click the **Power** tab.
3. Select **Power Save mode (laptops only)**.
4. Click **OK** to accept changes and close the dialog box.

Now, when your laptop is running on battery power, VIPRE will not check for updates or run scheduled scans.

3 Scanning your Computer

About Scans

Generally, a scan consists of VIPRE reading your computer's drive(s), determining what a threat is, and then either removing or quarantining that threat. VIPRE uses three types of scans:

- A **Quick Scan** will scan commonly affected areas of your computer. This scan is usually shorter in duration than the Deep Scan.
- A **Deep Scan** will perform a thorough scan of all areas of your computer. Depending on the amount of data on your hard drive, this could take longer.
- A **Custom Scan** is a targeted scan for very specific areas and/or types of items that you want VIPRE to look at, including running processes, registry files, cookies, and particular drives and folders.

How a scan can be triggered:

Manually

A **Manual scan** is a scan that you perform as needed. If you feel you your computer may be infected or just want to ensure that it isn't, running a manual scan will allow you to protect your computer.

See Scanning your computer for more information.

Automatically (scheduled scans)

A **scheduled scan** can be any of the three scan types that you schedule to run at a time of your choosing. By default, VIPRE is set to run a scheduled Deep Scan at 1:00 am. If your computer is not on during that time, you should change that time to one more suitable. You can add as many scheduled scans as you want.

See Scheduling Scans and Configuring Power Save Options for more information.

Email protection

Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything.

See About Email Protection and Configuring Email Protection for more information.

Command Line Scanner

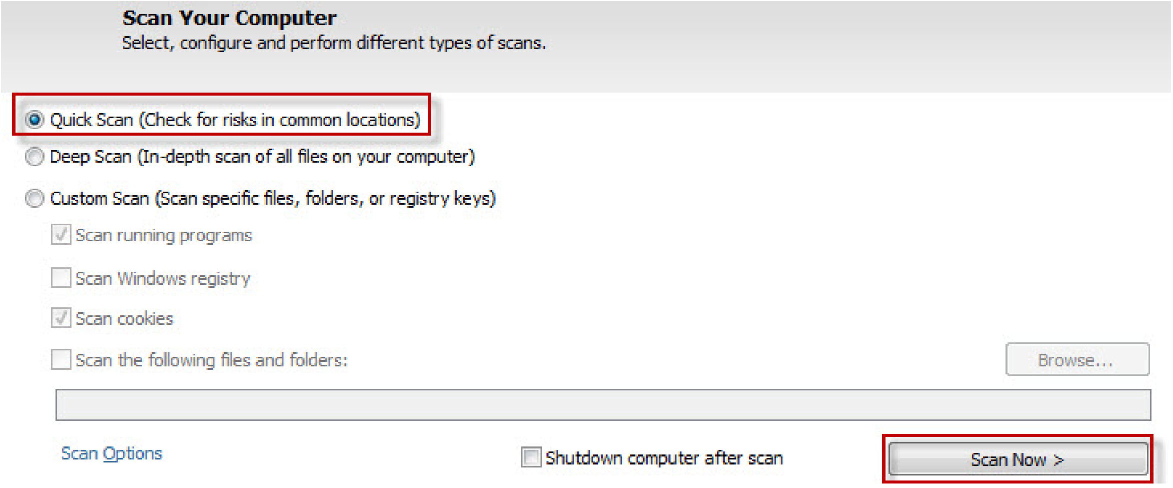
The **Command Line Scanner** is a helpful tool for the extreme occurrence that your computer becomes so infected from malware that it could become quite difficult to open any program, including VIPRE.

See Running the Command Line Scanner for more information.

Scanning your computer

VIPRE offers several options to configure and scan your computer.

> **Notes:** You can continue to use other VIPRE features while running a scan.
> If you cancel a scan, you can clean what the scan has found at that point.


Scan Your Computer

Select, configure and perform different types of scans.

- ● Quick Scan (Check for risks in common locations)
- ○ Deep Scan (In-depth scan of all files on your computer)
- ○ Custom Scan (Scan specific files, folders, or registry keys)
  - ☑ Scan running programs
  - □ Scan Windows registry
  - ☑ Scan cookies
  - □ Scan the following files and folders:

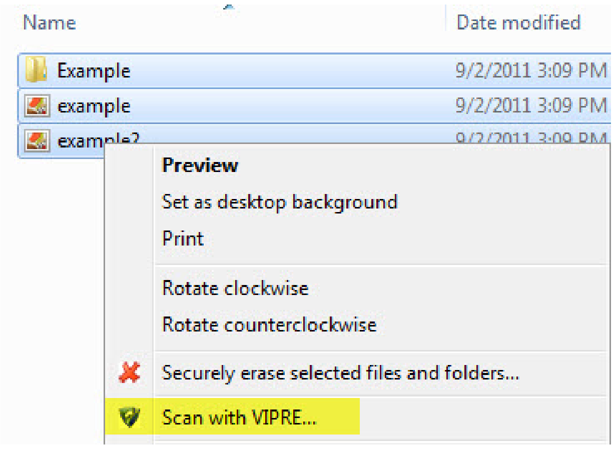
Screenshot 19: Scan screen

To run a simple scan:

1. Click the **Scan** tab. The Scan screen displays.
2. Select **Quick Scan**.
3. Click **Scan Now**. During the scan, the progress of the scan displays.
4. (If applicable) Once the scan completes, click **Clean**. VIPRE cleans the risks based on the recommended clean action listed in the Clean Action column.
5. Click **Done**.

To scan from the right-click menu:

You can scan one or more files from Windows Explorer from the right-click menu. When VIPRE installs on your computer, it puts an option in the right-click menu to run a scan.

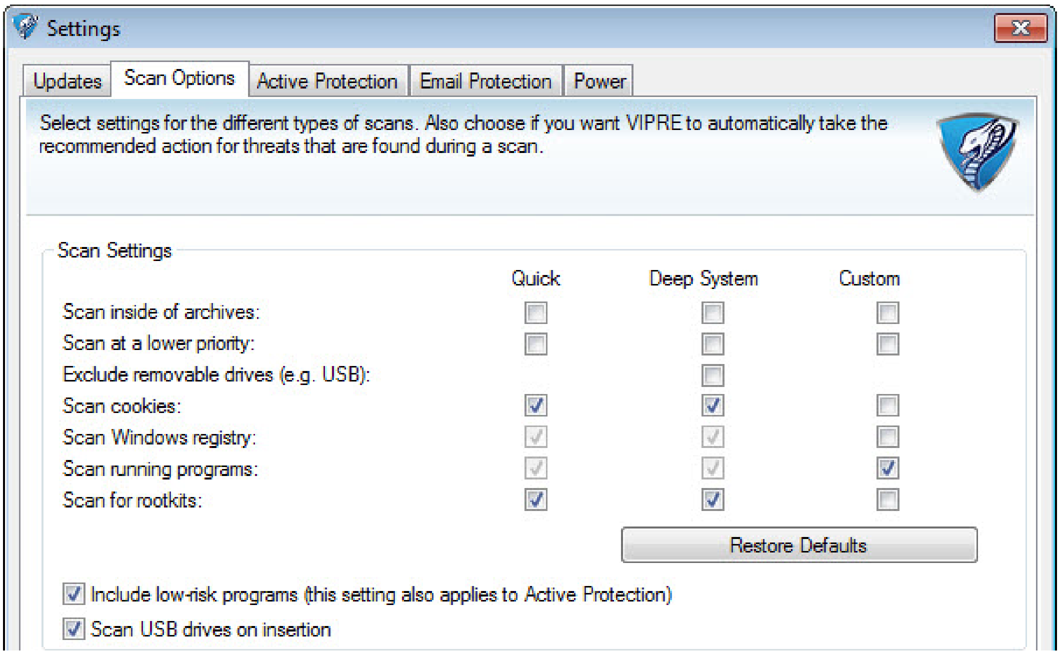


Screenshot 20: Right-click scan in Windows Explorer

After the scan is performed, the VIPRE Interface will open with your scan results.

Configuring Scan Options

Optionally, you can configure several ways how VIPRE runs a scan, or when you run a scan, you can simply rely on the default settings.



Select settings for the different types of scans. Also choose if you want VIPRE to automatically take the recommended action for threats that are found during a scan.

Scan Settings

	Quick	Deep System	Custom
Scan inside of archives:	□	□	□
Scan at a lower priority:	□	□	□
Exclude removable drives (e.g. USB):		□	
Scan cookies:	☑	☑	□
Scan Windows registry:	☑	☑	□
Scan running programs:	☑	☑	☑
Scan for rootkits:	☑	☑	□

☑ Include low-risk programs (this setting also applies to Active Protection)

☑ Scan USB drives on insertion

Screenshot 21: Scan Options

To configure scan options:

1. From the VIPRE menu, select **File>Settings**.
2. Click the **Scan Options** tab.
3. In the **Scan Settings** area, select any of the following for each of the three scan types:

- **Scan inside of archives**: Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined. See Working with Quarantined Items for more information.
- **Scan at a lower priority**: Select for VIPRE to operate at a lower priority, allowing you to continue working with other programs without decreased performance. It's good to select this option for scheduled scans that occur during times of regular use of the computer.
- **Exclude removable drives**: Select to exclude external or temporary drives, such as flash and USB drives or external hard drives. It's best to keep this selected all times, except when you are intentionally scanning those external drives. By default, Quick and Custom scans will automatically exclude these drives.
- **Scan cookies**: Select to include all cookies on your system. This only applies to Internet Explorer (IE).
- **Scan Windows registry**: Select for the scan to include your system's registry.
- **Scan running processes**: Select for the scan to include any program that is currently running. For example, if you have an Internet browser and an email program open, your scan will include these running programs. If unselected, VIPRE will not scan running programs.
- **Scan for rootkits**: Select to include rootkits (software tools intended to conceal running processes, files or system data from the operating system).

- **Include low-risk programs**: Select to include low-risk programs. This option applies to all scan types and Active Protection.
- **Scan USB drives on insertion**: Select to scan a USB drive once inserted into a USB slot. If VIPRE is currently scanning and a USB drive is inserted, you will be prompted to:
  - **Cancel the current scan and scan your USB drive**: Select to cancel the current scan. You will need to continue or restart the scan later after the USB scan completes.
  - **Continue the current scan and disregard scanning the USB drive**: Select to continue the current scan unchanged. If you want to scan the USB drive after the scan that is in progress, you will have to scan it manually.

> **Note:** You can click **Restore Defaults** to revert back to factory settings.

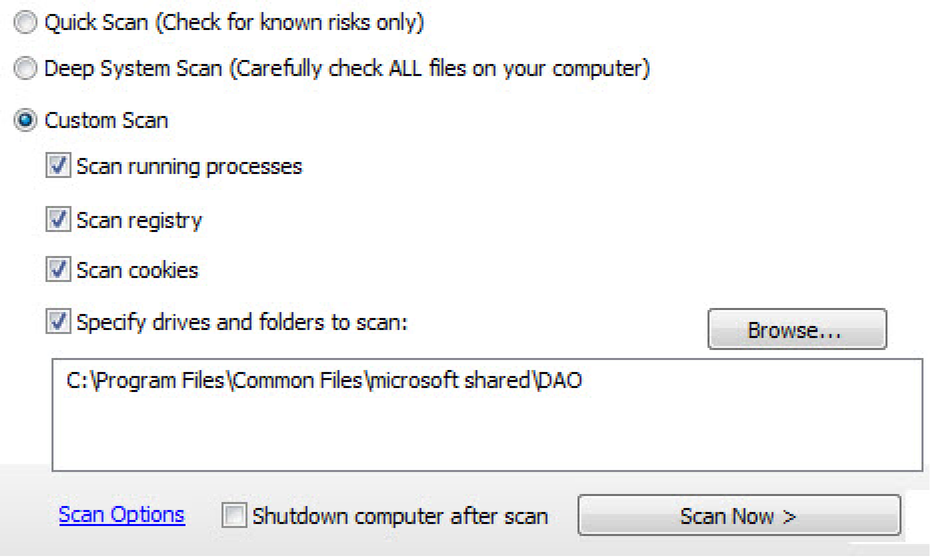
4. Optionally, change the default Action to take for scans.
5. Click **OK** to save your settings and close the dialog box.

Configuring and Running a Custom Scan

Configure **Custom Scan** options to scan specific areas of your computer.

To configure and run a Custom Scan:

1. Click the **Scan** tab. The Scan screen displays.
2. Select the **Custom Scan** option.



○ Quick Scan (Check for known risks only)

○ Deep System Scan (Carefully check ALL files on your computer)

● Custom Scan

☑ Scan running processes

☑ Scan registry

☑ Scan cookies

☑ Specify drives and folders to scan:

C:\Program Files\Common Files\microsoft shared\DAO

□ Shutdown computer after scan

Screenshot 22: Custom Scan options

3. Select any of the following options:

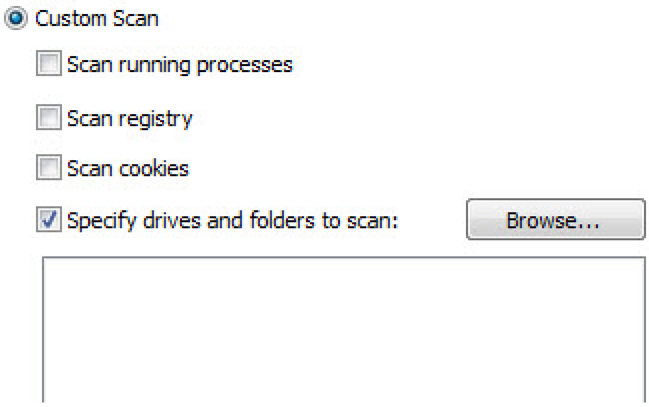
- **Scan running processes**: Select for the scan to include any program that is currently running. For example, if you have an Internet browser and an email program open, your scan will include these running programs. If unselected, VIPRE will not scan running programs.
- **Scan Windows registry**: Select for the scan to include your system's registry.
- **Scan cookies**: Select to include all cookies on your system. This only applies to Internet Explorer (IE).

- **Specify drives and folders to scan**: Select and then click **Browse** to perform a custom scan that includes a focus on specific drives, folders, and/or specific files.. (see "To specify drives and folders to scan" below)

4. Optionally, select **Shutdown computer after scan** to have VIPRE automatically shut down your computer after the scan completes.
5. Click **Scan Now**. Your selected scan starts. The Scan Progress screen displays allowing you to view the progress of the scan, pause the scan, or cancel it.

To specify drives and folders to scan:

1. Select **Specify drives and folders to scan**.



● Custom Scan

□ Scan running processes

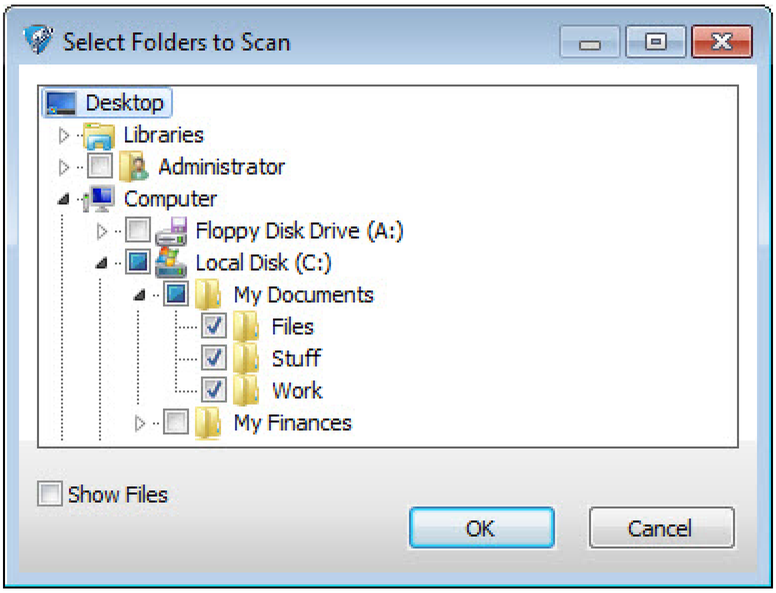
□ Scan registry

□ Scan cookies

☑ Specify drives and folders to scan:

Screenshot 23: Custom scan folder option

2. Click **Browse** and select the desired folders to scan.



- Desktop
  - Libraries
  - □ Administrator
  - Computer
    - □ Floppy Disk Drive (A:)
    - ■ Local Disk (C:)
      - ■ My Documents
        - ☑ Files
        - ☑ Stuff
        - ☑ Work
      - □ My Finances

□ Show Files

Screenshot 24: Selecting drives and folders

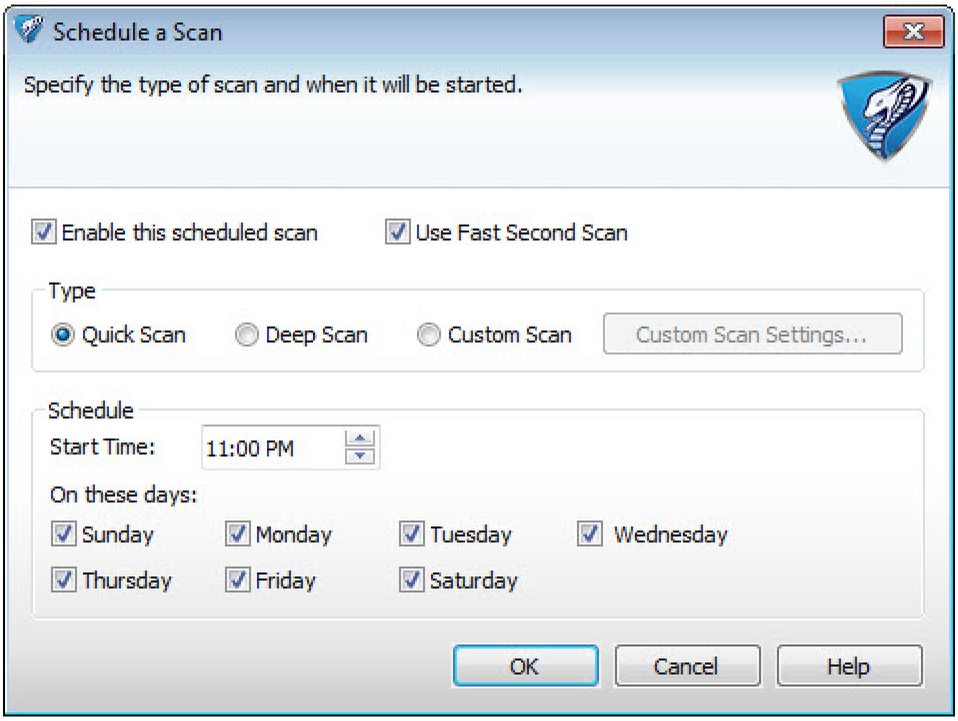
3. Optionally, select **Show Files** to display files within folders.
4. Click **OK**. The dialog box closes, and your selections display in the **Specify drives and folders to scan** list box.

Scheduling Scans

Create scheduled scans to ensure that VIPRE scans your computer regularly according to how often your computer is used. For example, if your computer is used every day, you should at least run a **Quick Scan** every day. We recommend that you schedule a **Deep Scan** to run in the middle of the night, provided your computer is turned on at that time.

To create a scheduled scan:

1. Open **Manage>Schedule Scans**.
2. Click **Add New**. The **Schedule a Scan** dialog box displays.



Schedule a Scan

Specify the type of scan and when it will be started.

☑ Enable this scheduled scan ☑ Use Fast Second Scan

Type

● Quick Scan ○ Deep Scan ○ Custom Scan [Custom Scan Settings...]

Schedule

Start Time: 11:00 PM

On these days:

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

Screenshot 25: Schedule a scan

3. Ensure **Enable this scheduled scan** is selected.
4. Optionally, select **Use Fast Second Scan** to make scans after the first scan faster.
5. Select one of the following:

   - A **Quick Scan** will scan commonly affected areas of your computer. This scan is usually shorter in duration than the Deep Scan.
   - A **Deep Scan** will perform a thorough scan of all areas of your computer. Depending on the amount of data on your hard drive, this could take longer.
   - A **Custom Scan** is a targeted scan for very specific areas and/or types of items that you want VIPRE to look at, including running processes, registry files, cookies, and particular drives and folders.

   > **IMPORTANT**: If you are scheduling a custom scan, it's important to click **Custom Scan Settings** and configure the scheduled custom scan.

6. Select a scan time. You can select the hours, minutes, or AM/PM, and then click the up or down arrows to choose your desired time.

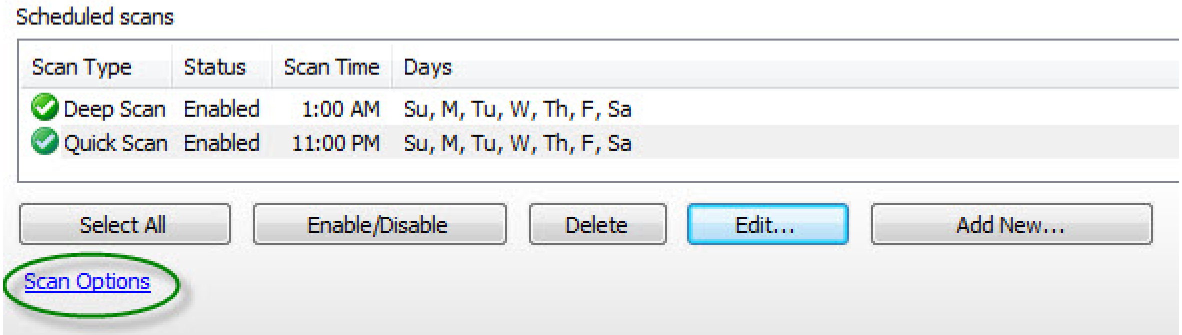
   > **Warning**: When adding a new scheduled scan, ensure that you do not turn off the "Wake from sleep on scheduled scans" in the power settings. This can affect automatic scans while a computer is in "sleep mode."

7. Select the days on which you wish to run the scan. You can select one or more days to be scanned. Deselect a day's box to remove it from the schedule.
8. Click **OK** to save changes. The dialog box closes and the scheduled scan displays on the Schedule Scans screen.
9. Optionally, configure Missed Scheduled Scans.
10. To schedule another scan, repeat steps 2 - 8.

To make up missed Scheduled Scans

If your computer is turned off at the time of a scheduled scan, you can set VIPRE to automatically make up a missed scan:

1. From the **Schedule Scans** screen, click the **Scan Options** link. The Scan Options screen displays.

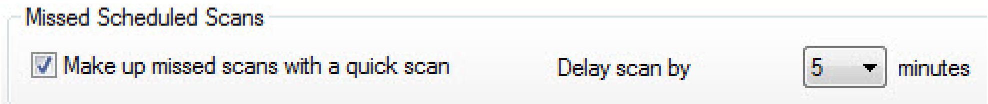


Scheduled scans

Scan Type	Status	Scan Time	Days
✓ Deep Scan	Enabled	1:00 AM	Su, M, Tu, W, Th, F, Sa
✓ Quick Scan	Enabled	11:00 PM	Su, M, Tu, W, Th, F, Sa

Screenshot 26: Schedule scans

2. In the **Missed Scheduled Scans** area, select the following:



Missed Scheduled Scans

☑ Make up missed scans with a quick scan   Delay scan by 5 minutes

Screenshot 27: Missed scheduled scans

- **Make up missed scans with a quick scan**: Select to automatically make up a missed scheduled scan. This means, for example, that if you scheduled a scan for 1:00 a.m. and the computer was turned off for the night, once your computer is turned on VIPRE will automatically begin a Quick scan after the delay.

> **Note**: Even if the missed scheduled scan was a Deep Scan, this make up scan will only be a Quick Scan.

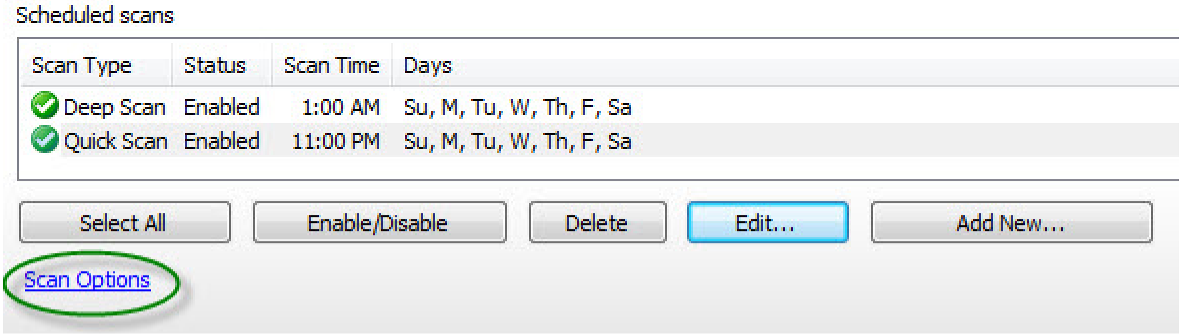
- **Delay scan by**: Select a number of minutes for VIPRE to wait before starting an automatic Quick scan. The default is 5 minutes.

3. Click **OK** to apply and save your settings. The dialog box closes and you are returned to the Schedule Scans screen.

To set the action for Scheduled Scans

You can set the cleaning action that VIPRE takes after running a scheduled scan.

1. From the **Schedule Scans** screen, click the **Scan Options** link. The Scan Options screen displays.

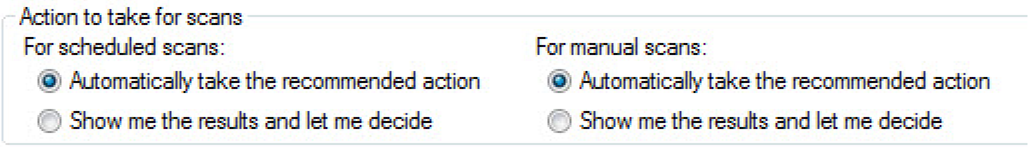


Scheduled scans

Scan Type	Status	Scan Time	Days
✓ Deep Scan	Enabled	1:00 AM	Su, M, Tu, W, Th, F, Sa
✓ Quick Scan	Enabled	11:00 PM	Su, M, Tu, W, Th, F, Sa

Screenshot 28: Schedule scans

2. In the **Action to take for scans** area, select one of the following for both scheduled and manual scans:



Action to take for scans

For scheduled scans:
● Automatically take the recommended action
○ Show me the results and let me decide

For manual scans:
● Automatically take the recommended action
○ Show me the results and let me decide

Screenshot 29: Actions for scans

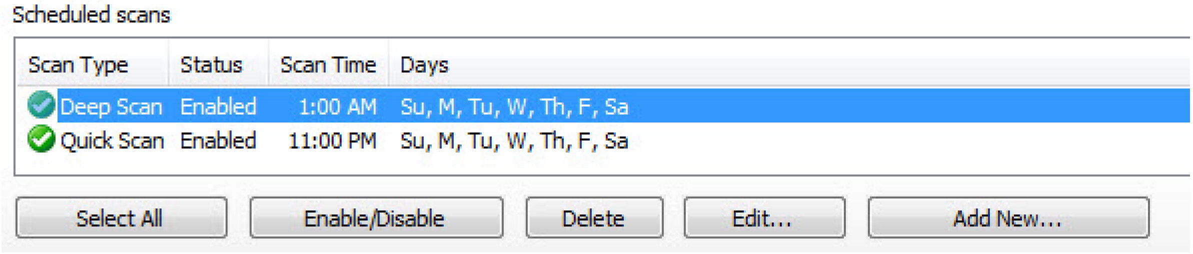
- **Automatically take the recommended action**: After a scheduled scan completes, VIPRE automatically cleans the risks based on the recommendation of GFI Software's research team, and will display the Clean Results screen for you to review the results. Select this option for the most carefree way of ridding your computer of malware.
- **Show me the results and let me decide**: After a scheduled scan completes, VIPRE displays the Review Risks Found screen for you to take corrective action on the detected risks. Select this option for the most control over your computer.

3. Click **OK** to apply and save your settings. The dialog box closes and you are returned to the Schedule Scans screen.

To edit an existing scheduled scan

From the Schedule Scans screen you can enable/disable, delete, and edit the a scan.

1. Open **Manage>Schedule Scans.**
2. Select the scan you wish to modify by clicking on it in the **Schedule scans** list box.



Scheduled scans

Scan Type	Status	Scan Time	Days
✓ Deep Scan	Enabled	1:00 AM	Su, M, Tu, W, Th, F, Sa
✓ Quick Scan	Enabled	11:00 PM	Su, M, Tu, W, Th, F, Sa

Screenshot 30: Schedule scans

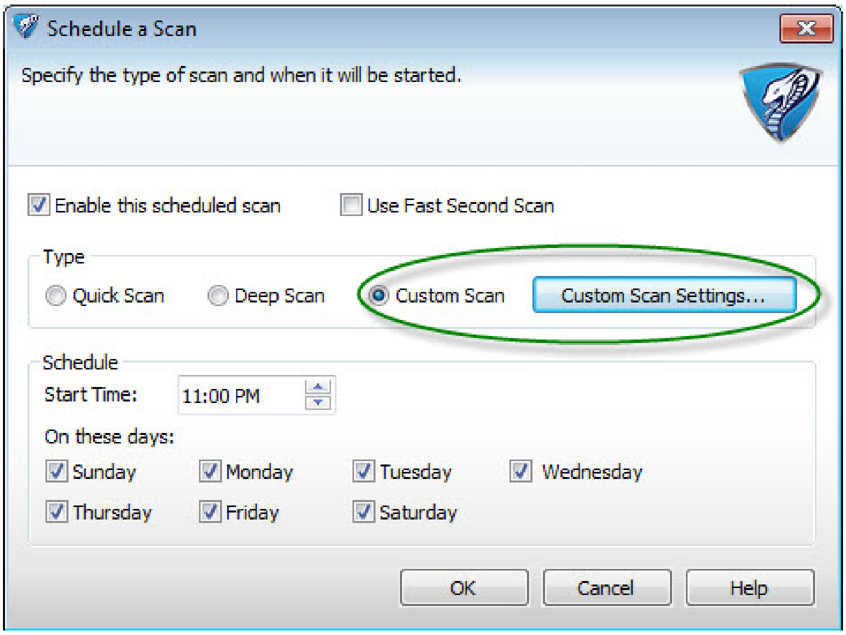
3. Perform any of the following:

- Click **Enable/Disable** to enable or disable the selected scan.
- Click **Delete** to delete the selected scan. If there is a scheduled scan that you no longer want to have scheduled, you can delete it.
- Click **Edit** to open the **Schedule a Scan** dialog box. Make any necessary changes and click **OK**.

> **Note:** Click **Select All** to perform a group action on all scheduled scans, such as deleting or enabling/disabling all scans. Clicking **Select All** disables the **Edit** function.

To configure Scheduled Custom Scans

1. Select the **Custom Scan** option and click **Custom Scan Options**.



Schedule a Scan

Specify the type of scan and when it will be started.

☑ Enable this scheduled scan □ Use Fast Second Scan

Type

○ Quick Scan ○ Deep Scan ● Custom Scan

Schedule

Start Time: 11:00 PM

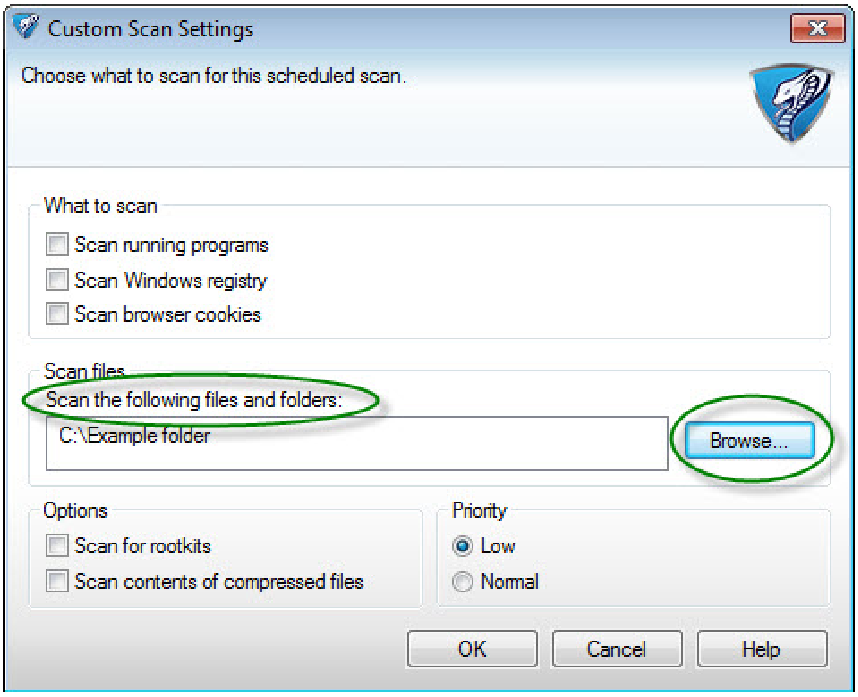
On these days:

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

Screenshot 31: Schedule a scan screen

The Custom Scan Settings dialog box displays.



Custom Scan Settings

Choose what to scan for this scheduled scan.

What to scan

□ Scan running programs

□ Scan Windows registry

□ Scan browser cookies

Scan files

Scan the following files and folders:

C:\Example folder

Browse...

Options

□ Scan for rootkits

□ Scan contents of compressed files

Priority

● Low

○ Normal

OK | Cancel | Help

Screenshot 32: Custom Scan Settings

2. Select any of the following options:

    - **Scan running processes**: Select for the scan to include any program that is currently running. For example, if you have an Internet browser and an email program open, your scan will include these running programs. If unselected, VIPRE will not scan running programs.
    - **Scan Windows registry**: Select for the scan to include your system's registry.
    - **Scan cookies**: Select to include all cookies on your system. This only applies to Internet Explorer (IE).
    - **Specify drives and folders to scan**: Select and then click **Browse** to perform a custom scan that includes a focus on specific drives, folders, and/or specific files.. (see "To specify drives and folders to scan")

3. Optionally select any of the additional **Options**:

    - **Scan for rootkits**: Select to include rootkits (software tools intended to conceal running processes, files or system data from the operating system).
    - **Scan inside of archives**: Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined. See Working with Quarantined Items for more information.
    - **Scan at a lower priority**: Select for VIPRE to operate at a lower priority, allowing you to continue working with other programs without decreased performance. It's good to select this option for scheduled scans that occur during times of regular use of the computer.

4. Click **OK** to save your settings and close the dialog box.

Running the Command Line Scanner (advanced)

VIPRE offers you the ability to run a scan and perform other functions from the command line scanner.

Note: Using VIPRE's command line scanner is an advanced feature and should only be used by knowledgeable computer users.

The following parameters are available for the command line scanner with the syntax: sbamcommandlinescanner.exe [parameter]:

Parameter	Description
/displaylocaldefversion	gets current version number of definitions
/displayVIPREversion	gets current VIPRE software version number
/displaysdkversion	gets current SDK version number
/scannowquick	starts a Quick scan
/scannowdeep	starts a Deep System scan
/updatedefs	starts update definition
/enableap	enables active protection
/applydefs [path to definitions]	applies definitions file from a saved location

To run VIPRE from the command line scanner:

1. Access the Windows Command Prompt. This can usually be opened by clicking the **Start** button and then selecting **All Programs>Accessories>Command Prompt**.
2. Verify that you are on the drive that VIPRE is installed.

   The default drive is C:.

3. Navigate to the VIPRE program folder.

   For example, cd Program Files\GFI Software\VIPRE Antivirus.

4. To display the valid syntax parameters, type sbamcommandlinescanner. The USAGE information is displayed, just as is displayed in the table above.
5. To run a parameter, type sbamcommandlinescanner.exe [parameter].

   For example, if you want to view the current version of VIPRE, type sbamcommandlinescanner.exe/displayVIPREversion.

Warning: Once you start a scan, do NOT manually attempt to terminate it. The scan MUST be allowed to complete to avoid config errors. You will receive a notification that the scan is running. Once the scan completes, you will receive the message "DONE:Cleaning Complete."

Note: Scans are run based on the default settings in the VIPRE interface. For example, if the Quick scan settings are set to: Include low-risk programs, Enable rootkit detection, and Scan cookies, then this is what the command line scanner will scan for when entering the /scannowquick command.

4 Managing Scan Results

Once a scan completes, VIPRE displays the **Review Risks Found** screen where you need to assign a clean action and clean the found risks. VIPRE's default is to clean with the Recommended Action.

Set a clean action and clean the found risks:

1. Click **Select All** to set an action to all listed risks.
   -or-
   Select one or more risks.
2. Under **Change Action to Take for selected items**, click the down arrow to pick from one of the following options:

   - **Recommended Action**: Allows VIPRE to determine the clean action for the selected risk based on the latest definitions that are installed on your computer.
   - **Quarantine/Disinfect**: Sets the Clean Action for the selected risk to **Quarantine**. VIPRE will first attempt to clean the infection in the file. If the file cannot be disinfected, VIPRE will place the infected file into Quarantine. It will stay in quarantine for a default of 15 days. On the 16th day, it will be automatically deleted. You can change the amount of time it stays in Quarantine from the Quarantine dialog box. The Quarantine gives you the opportunity to further evaluate this file before removing it from your computer permanently.
   - **Remove**: Sets the Clean Action for the selected risk to **Remove**. This setting removes the selected risk permanently from your computer, and is not the recommended action. It is better to **Quarantine** a risk first, giving you the opportunity to later restore it to your computer if it turns out to not be a risk to you.
   - **Allow**: Sets the Clean Action for the selected risk to **Allow**. This setting allows the selected risk to remain on your system. It will only be allowed just this one time. It may be detected again in future scans. If you believe this file to be acceptable to run on your computer, select **Allow Always**.
   - **Allow Always**: Sets the Clean Action for the selected risk to **Allow Always**. This setting allows the selected risk to always remain on your system and VIPRE will ignore it in future scans.

3. To set a restore point for system files that may have been detected as being infected, select **Create system restore point**.

   It is not uncommon for system files to become infected. Selecting this checkbox will enable the operating system to specify a system restore point prior to cleaning risks and deleting files. A System Restore is a Windows feature that allows you to undo harmful changes to your computer and restore it back to its original state just before the changes were made. For more information and accessing this Windows feature, go to **Start>Help and Support>**and locate **System Restore**. This restore point will be listed as "VIPRE clean action." **It is a good practice to always keep this selected**.

   > **Note:** This feature only restores system related files. It does not restore files and applications such as Hotbar.

4. Click **Clean Now**. The Clean Progress screen displays followed quickly by the Clean Results screen.

If necessary, you can click **Cancel** to cancel the clean action and clean the risks at a later time.

> **Note:** After the cleaning is finished, you may be prompted to reboot your machine for VIPRE's Boot Time Cleaner to completely remove a "hard to remove" risk.

Scan Progress Screen

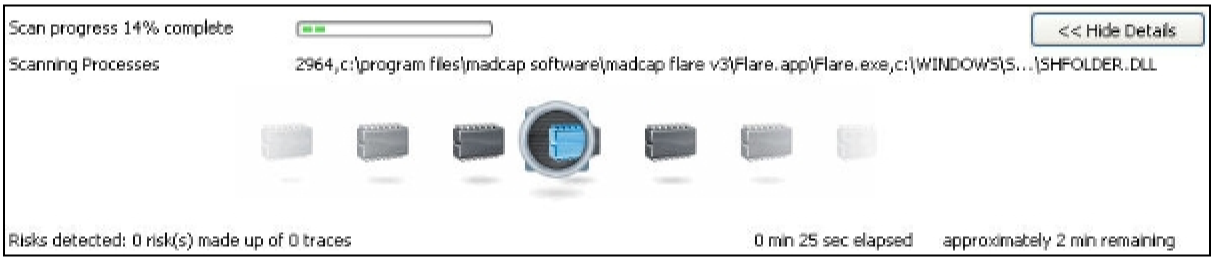
The **Scan Progress** screen displays once a scan is initiated and is used to monitor progress of the scan. Once risks are detected, they are displayed in the Risk list box below the Scan progress area. While a scan is running, you can **Pause/Resume** or **Cancel** it.

> **Note:** Once a scan completes, this screen automatically closes and is replaced by the Review Risks Found screen or the Clean Results screen.

This screen contains the following items:

Scan progress area

The Scan progress area displays all of the scanning information as it is detected in real-time.



Scan progress 14% complete

Scanning Processes 2964,c:\program files\madcap software\madcap flare v3\Flare.app\Flare.exe,c:\WINDOWS\S...\SHFOLDER.DLL

Risks detected: 0 risk(s) made up of 0 traces

0 min 25 sec elapsed

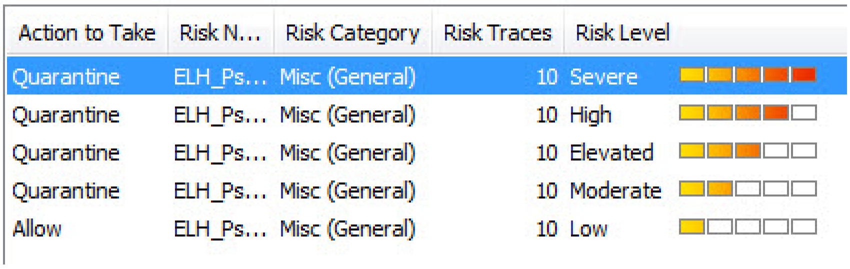
approximately 2 min remaining

Screenshot 33: Scan progress

- **Scan progress**: Displays the percentage of the scan complete.
- **Progress bar**: Graphically displays how much of the scan has been completed.
- **Hide Details/Show Details:** Hides or displays the scanning progress graphic. The image shows the type of item being scanned.
- **File path and name**: Displays the file path and filename of what is being scanned.
- **Risks detected**: Displays the number of risks detected at that moment and the number of traces.
- **Time elapsed**: Displays the amount of scan time that has elapsed.
- **Time remaining:** Displays the approximate time remaining for the scan.

Risk list box

The Risk list box displays a table of risks discovered during the scan. You can click on a column heading to sort by that column.



Action to Take	Risk N...	Risk Category	Risk Traces	Risk Level
Quarantine	ELH_Ps...	Misc (General)	10	Severe ■■■■■
Quarantine	ELH_Ps...	Misc (General)	10	High ■■■■□
Quarantine	ELH_Ps...	Misc (General)	10	Elevated ■■■□□
Quarantine	ELH_Ps...	Misc (General)	10	Moderate ■■□□□
Allow	ELH_Ps...	Misc (General)	10	Low ■□□□□

Screenshot 34: Risk list box

The table includes the following columns:

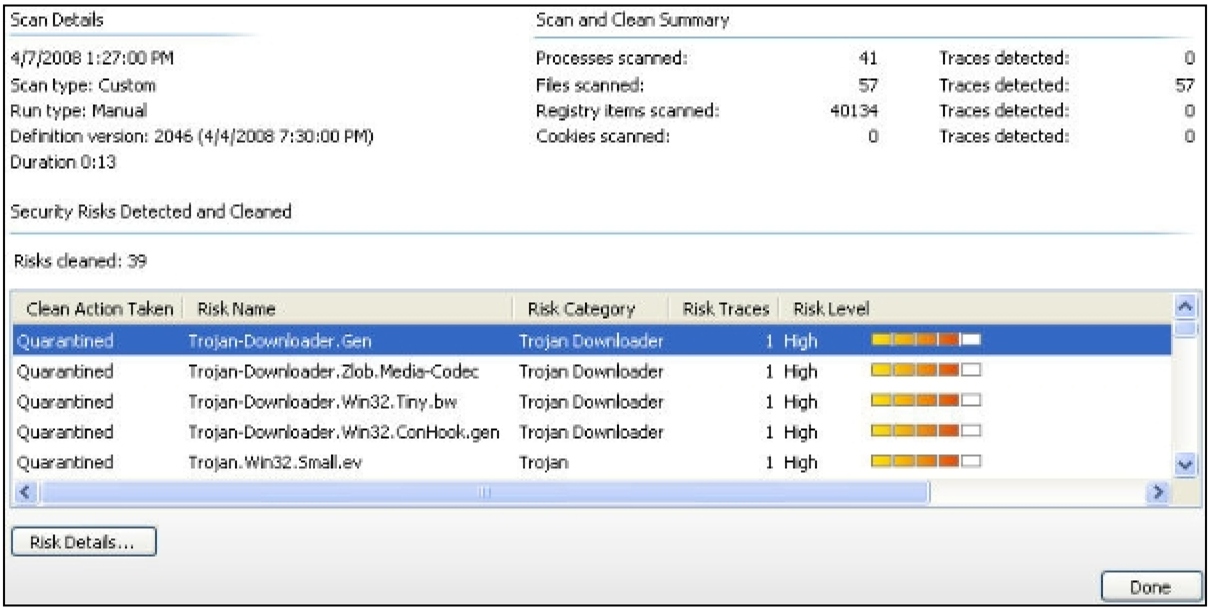
- **Action to Take**: Displays the action to be taken: Quarantined, Remove, Allow, or Allow Always.
- **Risk Name**: Displays the name of the risk that GFI uses to refer to this risk. Other security companies may use a different name.
- **Risk Category**: Displays the type (or category) of the risk (e.g. Adware, Trojan, Rootkit, Virus, Worm, Unknown Program, Misc., etc.).
- **Risk Traces**: Displays the number of traces of this risk that were detected.
- **Risk Level**: Displays the severity of the risk. You can use this as a general guide in determining what action to take for a particular risk. The risk levels include Low, Moderate, Elevated, High, and Severe. The level is accompanied by a color scale. The more boxes filled in by colors, the greater the risk and the greater the urgency of you acting on it.

Buttons

- **Pause**: Click to temporarily stop an ongoing scan. Once clicked, it changes to the **Resume** button.
- **Resume**: Click to continue a paused scan. (The **Resume** button is only displayed if the scan has been paused.)
- **Cancel**: Click to terminate the scan. You will be prompted to verify. Click **Yes** to continue with canceling the scan or **No** to stop the cancel. Canceling the scan returns you to the Scan screen.

Clean Results Screen

The **Clean Results** screen is displayed after a scan completes, and items detected have been cleaned. This screen is for informational purposes only, allowing you to view the cleaning actions that were taken and to view the risk details of a particular risk.



Scan Details

4/7/2008 1:27:00 PM
Scan type: Custom
Run type: Manual
Definition version: 2046 (4/4/2008 7:30:00 PM)
Duration 0:13

Scan and Clean Summary

Processes scanned:	41	Traces detected:	0
Files scanned:	57	Traces detected:	57
Registry items scanned:	40134	Traces detected:	0
Cookies scanned:	0	Traces detected:	0

Security Risks Detected and Cleaned

Risks cleaned: 39

Clean Action Taken	Risk Name	Risk Category	Risk Traces	Risk Level
Quarantined	Trojan-Downloader.Gen	Trojan Downloader	1	High ■■■■□
Quarantined	Trojan-Downloader.Zlob.Media-Codec	Trojan Downloader	1	High ■■■■□
Quarantined	Trojan-Downloader.Win32.Tiny.bw	Trojan Downloader	1	High ■■■■□
Quarantined	Trojan-Downloader.Win32.ConHook.gen	Trojan Downloader	1	High ■■■■□
Quarantined	Trojan.Win32.Small.ev	Trojan	1	High ■■■■□

Screenshot 35: Clean results

This screen contains the following items:

Scan Details

- **Date and time**: Displays the date and time the history event occurred.
- **Scan Type**: The type of scan that was run; either Quick, Deep System, or Custom.
- **Run Type**: Displays how the scan was initiated; either manual or automatic (scheduled).
- **Definition Version**: Displays the version of definitions that the scan was based on.
- **Scan Duration**: Displays how long the scan took in minutes and seconds.

Scan and Clean Summary

The **traces detected** displays how many traces were detected for the corresponding item to its left.

- **Processes scanned**: Displays the number of running processes that were scanned.
- **Files scanned**: Displays the number of files that were scanned.
- **Registry Items scanned**: Displays the number of items in your computer's registry that were scanned.
- **Cookies scanned**: Displays the number of cookies that were scanned.

Security Risks Detected and Cleaned

This section lists the total number of Risks cleaned. The table provides information on the risks detected during that scan and includes the following columns:

- **Clean Action Taken**: Displays the clean action that VIPRE took for the corresponding risk; either Quarantined, Removed, or Allowed. If no clean action is taken this column is left blank.
- **Risk Category**: Displays the type (or category) of the risk (e.g. Adware, Trojan, Rootkit, Virus, Worm, Unknown Program, Misc., etc.).
- **Risk Name**: Displays GFI Software's name of the known security risk.
- **Risk Traces**: Displays the number of traces found for the corresponding risk.
- **Security Risk Level**: Displays the severity of the risk. You can use this as a general guide in determining what action to take for a particular risk. The risk levels include Low, Moderate, Elevated, High, and Severe. The level is accompanied by a color scale. The more boxes filled in by colors, the greater the risk and the greater the urgency of you acting on it.

Buttons

- **Risk Details**: Selecting a risk and clicking **Risk Details** displays the **Risk Details** dialog box.
- **Done**: Closes the dialog box, returning you to the **Scan** screen.

> **Note:** After the cleaning is finished, you may be prompted to reboot your machine for VIPRE's Boot Time Cleaner to completely remove a "hard to remove" risk.

- **Cancel**: Click to cancel the clean action.

Sending Files to GFI for Analysis

If VIPRE quarantines a file that you believe should not be quarantined (for example, potential false positive), you can send it to GFI Software for analysis to help us improve our security risk database. You can send multiple files from the Quarantine screen or a single file from the Help menu.

> **Note**: Go to http://www.gfi.com/pages/privacy.htm to view GFI Software's privacy policy.

To send a file for analysis when restoring a file from quarantine (multiple files):

1. Open the **Quarantine** screen (click the **MANAGE** tab and then click **View quarantine**). The Quarantine screen displays a table of quarantined risks.
2. In the table of quarantined risks, locate and select the quarantined item(s) that you want to send to GFI.
3. Click **Restore from Quarantine**. The Unquarantine dialog box displays.
4. Select **Send files to GFI for analysis**.
5. Click **OK**. The "Files sent to GFI" dialog box displays a confirmation of the sent file(s).
6. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
7. Click **OK**.

To send a file for analysis from the quarantine risk area (multiple files):

1. Open the **Quarantine** screen (click the **MANAGE** tab and then click **View quarantine**). The Quarantine screen displays a table of quarantined risks.
2. In the table of quarantined risks, locate and select the quarantined item(s) that you want to send to GFI.
3. Right-click and select **Send to GFI**. The "Files sent to GFI" dialog box displays a confirmation of the sent file(s).
4. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
5. Click **OK**.

To send a file for analysis from a saved location (only one file):

1. From the **Help** menu, select **Send file for analysis**. The "Send a file to GFI Software" dialog box displays.
2. Click **Browse** and navigate to the file that you want to send for analysis. Click **Open**. The file is displayed under "File to send:".
3. Click **Send**. The "Send a file to GFI Software" dialog box closes and the "Files sent to GFI" dialog box displays a confirmation of the sent file(s).
4. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
5. Click **OK**.

Adding Always Allowed Items

There may be some items on your computer that you determine to be safe and do not want scanned. This is accomplished by adding it to the Always Allowed list. You can remove it from this list later.

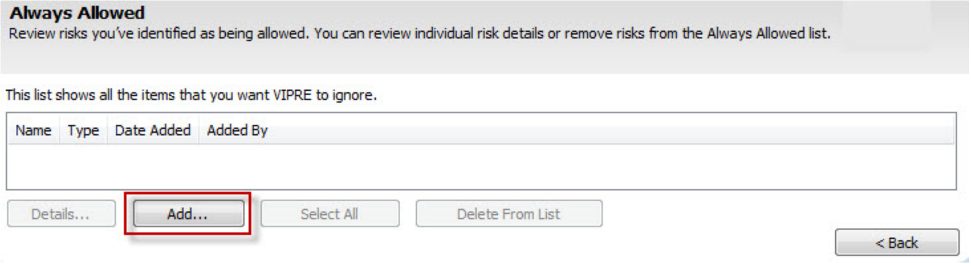
> **Note:** It is not necessary to list every file that you consider safe to this list. Use this only when VIPRE identifies items that you want to be allowed. For example, this could occur for some gambling programs and some third party ad programs that you may choose to run on your system.

To always allow a program to run on your computer after a scan:

1. Run a scan on your computer.
2. From the **Review Risks Found** screen, select the item you want to always be allowed.
3. Under **Change Action to Take for selected items**, click the down arrow Recommended Action ▾ and select **Allow Always.**
4. Click **Clean**. The selected item will be placed in the **Always Allowed** list and will no longer be identified as a risk during future scans.

   At any time, you can remove it from the list.

To always allow a program to run on your computer manually from the Always Allowed screen:



Always Allowed

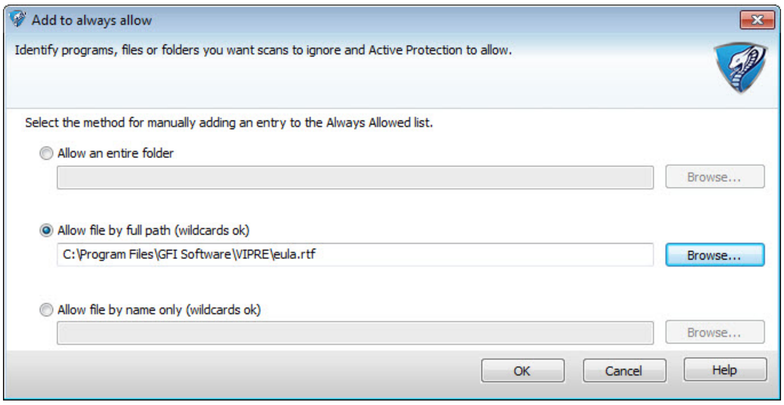
Review risks you've identified as being allowed. You can review individual risk details or remove risks from the Always Allowed list.

This list shows all the items that you want VIPRE to ignore.

Name	Type	Date Added	Added By

Screenshot 36: Always allowed screen

1. Click **Add**. The Add to always allow dialog box displays.
2. Select one of the following:



Add to always allow

Identify programs, files or folders you want scans to ignore and Active Protection to allow.

Select the method for manually adding an entry to the Always Allowed list.

○ Allow an entire folder

● Allow file by full path (wildcards ok)

C:\Program Files\GFI Software\VIPRE\eula.rtf

○ Allow file by name only (wildcards ok)

Screenshot 37: Add to always allow dialog box

- **Allow an entire folder**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. For example, C:\Example\. All files under this directory will be allowed. If any of the files or folder(s) exists elsewhere on your system, it will not apply to this always allowed selection.
- **Allow file by full path (wildcards ok)**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. For example, C:\-Example\example file.txt. Only the file with this path will be allowed. If the file exists elsewhere on your system, it will not apply to this always allowed selection. The supported wildcards are "*" and "?".
- **Allow by file name only (wildcards ok)**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. Use this field if AP or a scan is detecting a specific file frequently. For example Firefox.exe. Any file with this name will be allowed no matter where it exists on your system.

3. Click **OK**. The item is added to the Always Allowed list.

To view details of an Always Allowed item:

1. Open the **Always Allowed** screen by selecting **Manage** tab>**Always Allowed**.
2. Select on an item and click **Details**. The **Always Allowed Details** dialog box displays.
   -or-
   Double-click on a risk to display the **Always Allowed Details** dialog box.

To remove an allowed item from the Always Allowed list:

1. Open the **Always Allowed** screen by selecting **Manage** tab>**Always Allowed**.
2. Select the item you wish to remove and click **Remove From List**. The item is removed from the Always Allowed list and will show up during future scans or when it's run with AP is enabled.

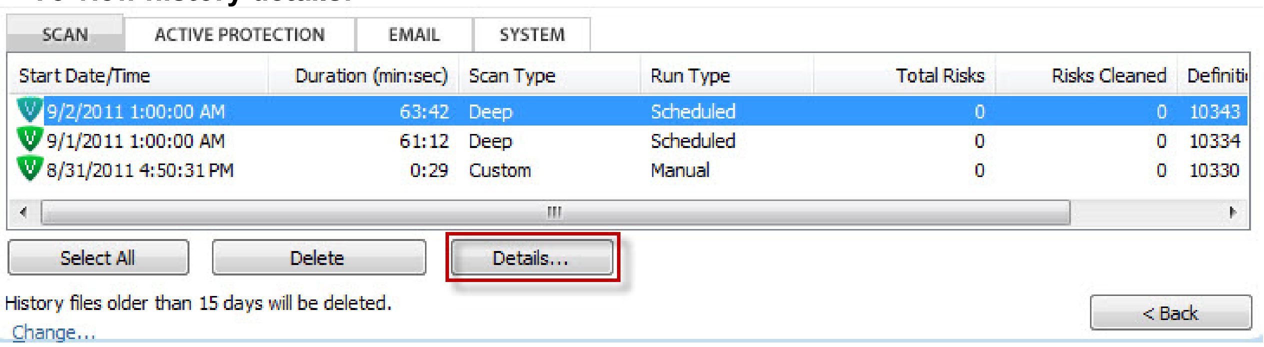
> **Note:** You can click **Select All** and then click **Remove From List** to remove all items from the **Always Allowed** list.

Working with History Events

Any action that occurs in VIPRE is recorded as a history, which includes scan, Active Protection (AP), Email, and System. You can view and delete the history. By default, the history is stored for 15 days. On the 16th day, the history is automatically deleted. You can change the number of days that VIPRE will keep the history and manually delete them.

To display the **View History** screen, select **Manage tab**>**History**.

To view history details:



Start Date/Time	Duration (min:sec)	Scan Type	Run Type	Total Risks	Risks Cleaned	Definiti
9/2/2011 1:00:00 AM	63:42	Deep	Scheduled	0	0	10343
9/1/2011 1:00:00 AM	61:12	Deep	Scheduled	0	0	10334
8/31/2011 4:50:31 PM	0:29	Custom	Manual	0	0	10330

History files older than 15 days will be deleted.
Change...

Screenshot 38: View scan history screen

1. Select either the **Scan**, **Active Protection**, **Email**, or **System** tab.
2. Select the history (row) you wish to review.
3. Click **Details**. The dialog box for the corresponding history displays.

To automatically delete VIPRE history:

Performing this procedure will affect the history under Active Protection (AP), email, and system—all at once.

1. Click the **Change** link. The History Options dialog box displays.
2. Ensure the **Delete history older than** option is selected.
3. Click the up or down arrows to set the number of days you wish to keep histories.
   -or-
   Click inside the combo-box and enter the number of days (1-365) you wish to keep histories.

> **Note:** Selecting the **Keep all of my history** option disables the auto-delete function. All histories will be kept until you manually delete them.

4. Click **OK** to save changes and close the dialog box.

To delete an history item:

From either the Scan, Active Protection, or Email tabs, select the item (row) you wish to delete and click **Delete**.

> **Note:** You can click **Select All** and then click **Delete** to clear the whole list for that tab only. The System tab allows you to remove all of its items by clicking **Clear All**.

Quarantined Items

The Quarantine is a safe place on your computer that VIPRE uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review its details and research it further, and then remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove it from Quarantine.

To work with **Quarantine** items, select **Manage tab>Quarantine** and continue with any of the following procedures:

To view the details of a risk:

1. Select a risk from the list and click **Risk Details**. The **Risk Details** dialog box displays.
   -or-
   Double-click on a risk to display the **Risk Details** dialog box.
2. Optionally, click **Learn More** for additional information.

To restore a risk from the quarantine list:

Select the risk(s) to restore and click **Restore from Quarantine**. The Unquarantine dialog box displays.

To delete a quarantined item from your computer:

Select the risk you wish to delete and click **Delete from Computer**. The item is permanently removed from your computer.

Note: You can click **Select All** and then click **Delete from Computer** to delete all items in Quarantine from your computer.

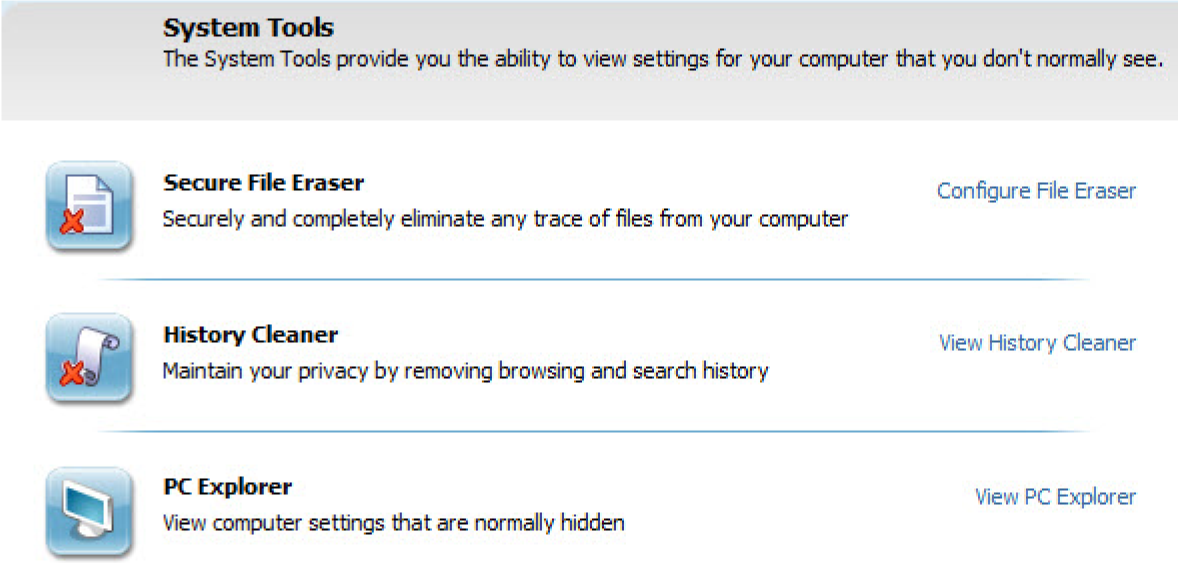
To set the auto delete function:

1. Click the **Change** link. The **Quarantine** dialog box displays.
2. Ensure the **Delete quarantined items older than** option is selected.
3. Click the up or down arrows to set the number of days you wish to keep quarantined items and click **OK**.
   -or-
   Click inside the box and manually enter the number of days you wish to keep quarantined items and click **OK**.

Note: Selecting the **Never automatically delete quarantined items** option disables the auto-delete function. All quarantined items will be kept until you manually delete them.

5 Using System Tools

The **System Tools** screen provides you access to areas of your computer that you don't normally see.



System Tools

The System Tools provide you the ability to view settings for your computer that you don't normally see.

Secure File Eraser

Securely and completely eliminate any trace of files from your computer

History Cleaner

Maintain your privacy by removing browsing and search history

PC Explorer

View computer settings that are normally hidden

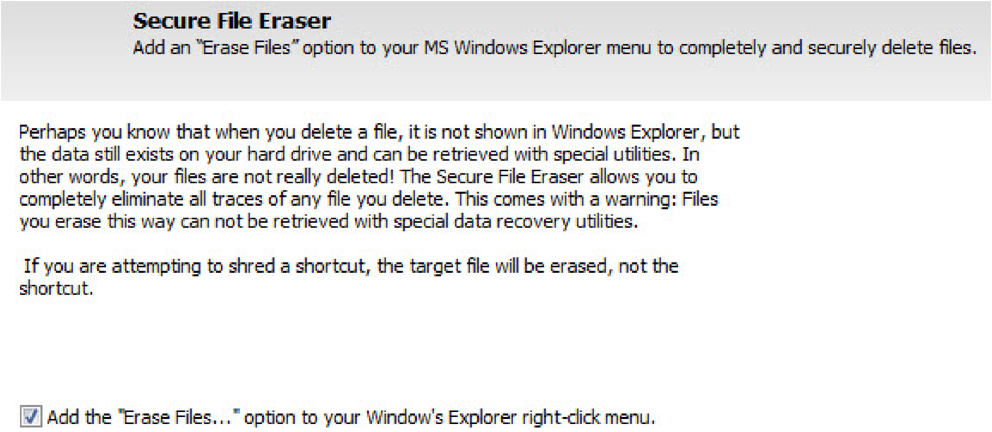
- The **Secure File Eraser** allows you to completely eliminate all traces of a file.
- The **History Cleaner** is a privacy tool that allows you to remove your browsing and search histories, including the history stored by many popular applications.
- The **PC Explorer** allows you to view settings on your computer that are normally hidden and add programs to the Always Allowed list.

Erasing Files Permanently

VIPRE offers you a privacy tool to permanently remove files from a storage device. When a file is deleted, it is not really gone. While the file is no longer shown in Windows Explorer, the data still exists on the drive and can be retrieved with special utilities. The **Secure File Eraser** allows you to completely eliminate all traces of a file.

Warning: When you use the Secure File Eraser to erase a file, the file cannot be retrieved with special data recovery utilities. If you are attempting to remove a shortcut, the target file will be permanently erased, NOT the shortcut.

Note: You can permanently erase files from nearly any drive (storage device) connected to your computer. For example, floppy drives, flash drives, external and internal hard drives. Both 32- and 64-bit are supported.



Secure File Eraser

Add an "Erase Files" option to your MS Windows Explorer menu to completely and securely delete files.

Perhaps you know that when you delete a file, it is not shown in Windows Explorer, but the data still exists on your hard drive and can be retrieved with special utilities. In other words, your files are not really deleted! The Secure File Eraser allows you to completely eliminate all traces of any file you delete. This comes with a warning: Files you erase this way can not be retrieved with special data recovery utilities.

If you are attempting to shred a shortcut, the target file will be erased, not the shortcut.

☑ Add the "Erase Files..." option to your Window's Explorer right-click menu.

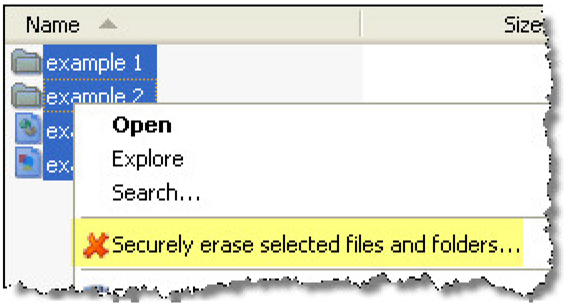
Screenshot 39: Secure file eraser setting

To permanently erase a file from a storage device:

1. Click on the **Tools** tab, and then click the **Secure File Eraser** icon. The Secure File Eraser screen displays.
2. Select the **Add the "Erase files..." option to your Windows Explorer right-click menu** checkbox. This option will be immediately added to the Window's Explorer menu, allowing you to use this feature.
3. Open **Windows Explorer**.

> **Tip:** To open Windows Explorer on your computer, right-click on **Windows Start** and select **Explore**.

4. In **Windows Explorer**, navigate to the desired drive, folder, and/or file and select one or more items to be permanently removed.
5. Right-click on the selected items. The options menu displays.



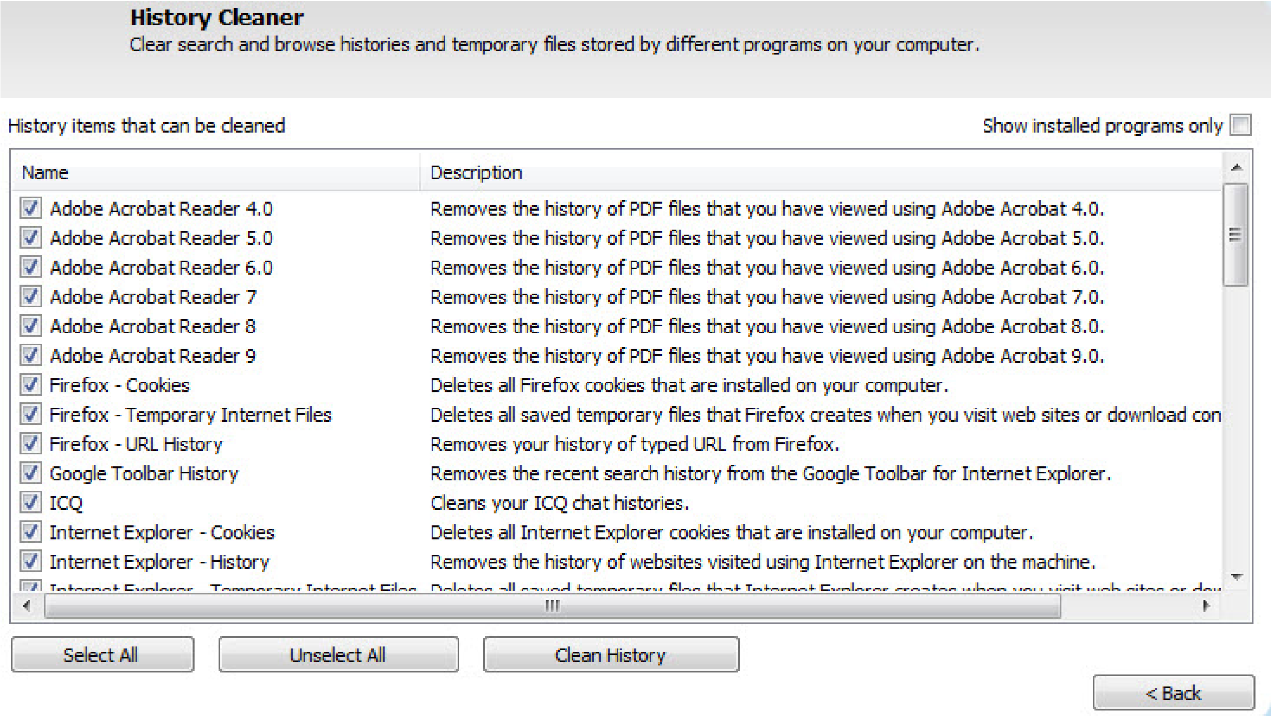
Screenshot 40: Example to securely erase files and folders by right-click menu

6. Select **Securely erase selected files and folders...** The confirmation window displays.
7. Click **Yes**. The selected items are permanently removed from the drive.

> **Note:** Depending on the size and quantity of selected files, you may experience a short delay before you see them removed.

Removing Browsing and Search Histories from your Computer

You can remove browsing and search histories from your computer, including the history stored by many popular applications.



History Cleaner

Clear search and browse histories and temporary files stored by different programs on your computer.

History items that can be cleaned

Show installed programs only □

Name	Description
☑ Adobe Acrobat Reader 4.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 4.0.
☑ Adobe Acrobat Reader 5.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 5.0.
☑ Adobe Acrobat Reader 6.0	Removes the history of PDF files that you have viewed using Adobe Acrobat 6.0.
☑ Adobe Acrobat Reader 7	Removes the history of PDF files that you have viewed using Adobe Acrobat 7.0.
☑ Adobe Acrobat Reader 8	Removes the history of PDF files that you have viewed using Adobe Acrobat 8.0.
☑ Adobe Acrobat Reader 9	Removes the history of PDF files that you have viewed using Adobe Acrobat 9.0.
☑ Firefox - Cookies	Deletes all Firefox cookies that are installed on your computer.
☑ Firefox - Temporary Internet Files	Deletes all saved temporary files that Firefox creates when you visit web sites or download con
☑ Firefox - URL History	Removes your history of typed URL from Firefox.
☑ Google Toolbar History	Removes the recent search history from the Google Toolbar for Internet Explorer.
☑ ICQ	Cleans your ICQ chat histories.
☑ Internet Explorer - Cookies	Deletes all Internet Explorer cookies that are installed on your computer.
☑ Internet Explorer - History	Removes the history of websites visited using Internet Explorer on the machine.
☑ Internet Explorer - Temporary Internet Files	Deletes all saved temporary files that Internet Explorer creates when you visit web sites or dow

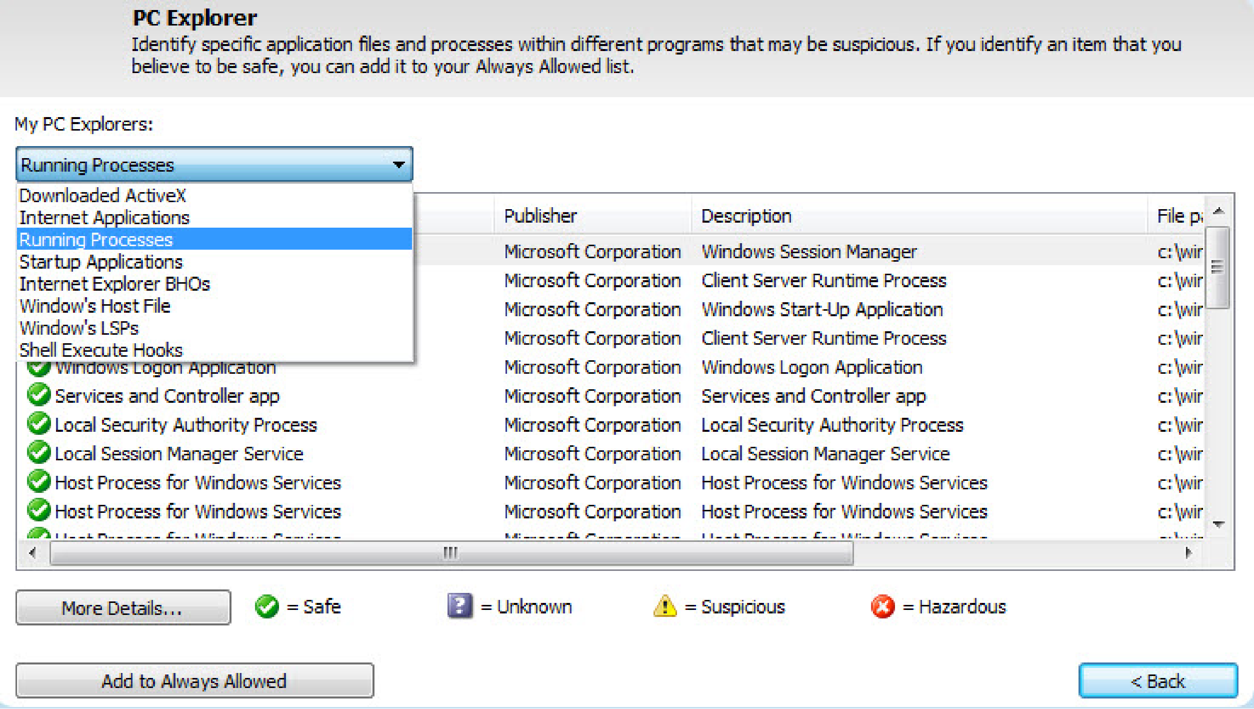
Screenshot 41: History cleaner settings

To permanently remove browsing and search history from your computer:

1. Click the **Tools** tab, and then click **History Cleaner**. The History Cleaner screen displays.
2. To display only programs installed on your machine, select **Show installed programs only**.
   -or-
   To view a listing of all programs that VIPRE can clean, deselect **Show installed programs only**.
3. In the list, select the checkboxes for the program that you want cleaned.
   -or-
   Click **Select All** to select all programs for cleaning.
   -or-
   Click **Unselect All** to deselect all programs from the list.
4. Click **Clean History**. VIPRE cleans the histories of all select programs and displays a message when finished.
5. Click **OK**.

Using PC Explorers

VIPRE's PC Explorers allows you to view settings on your computer that are normally hidden, and add programs to your Always Allowed list.



PC Explorer

Identify specific application files and processes within different programs that may be suspicious. If you identify an item that you believe to be safe, you can add it to your Always Allowed list.

My PC Explorers: Running Processes

	Publisher	Description	File pa
	Microsoft Corporation	Windows Session Manager	c:\wir
	Microsoft Corporation	Client Server Runtime Process	c:\wir
	Microsoft Corporation	Windows Start-Up Application	c:\wir
	Microsoft Corporation	Client Server Runtime Process	c:\wir
✓ Windows Logon Application	Microsoft Corporation	Windows Logon Application	c:\wir
✓ Services and Controller app	Microsoft Corporation	Services and Controller app	c:\wir
✓ Local Security Authority Process	Microsoft Corporation	Local Security Authority Process	c:\wir
✓ Local Session Manager Service	Microsoft Corporation	Local Session Manager Service	c:\wir
✓ Host Process for Windows Services	Microsoft Corporation	Host Process for Windows Services	c:\wir
✓ Host Process for Windows Services	Microsoft Corporation	Host Process for Windows Services	c:\wir

Screenshot 42: PC explorers screen

To view the PC Explorers:

1. Select **Tools>PC Explorer** tab. The System Tools screen displays.
2. From the **My PC Explorers drop-down box**, select from one of the following:
    - **Downloaded ActiveX**: Displays all the downloaded and currently installed ActiveX programs for Internet Explorer.
    - **Internet Applications**: Displays a list of programs that are currently connected to a remote computer, or are listening for connections from a network or the Internet.
    - **Running Processes**: Displays a list of all the processes (programs) that are currently running on your computer.
    - **Startup Programs**: Displays a list of all the applications that can start up and run when you start your computer or log into Windows.
    - **Internet Explorer BHOs**: Also known as "Browser Helper Objects," this is an application that extends Internet Explorer and acts as a plug-in.
    - **Window's Host File**: Displays a list of the current host files in your Windows Host file.
    - **Window's LSPs**: Also known as "Winsock Layered Service Providers," this shows all Layered Service Providers that are installed on your computer.
    - **Shell Execute Hooks**: Allows you to view any of your computer's Windows Shell Execute Hooks.
3. Select an item in the list and click **More Details** or double-click on the selected item. The PC Explorer Details dialog box displays with more information on the selected item.
4. Click **OK** to close the dialog box.

To add an item to the Always Allowed list:

If you find an item listed that is not "Safe" and you believe that it is, click **Add to Always Allowed** to add the program to your Always Allowed list.

> **Note:** Items that have the Safe icon ✓ are already always allowed.

6 Appendix I: Glossary

Adware

Adware, also known as advertising software, is often contextually or behaviorally based and tracks browsing habits in order to display third-party ads that are meant to be relevant to the user. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within Web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results.

Adware Bundler

An Adware Bundler is a downloadable program that is typically "freeware" because it is bundled with advertising software -- adware. The adware may function independently of the bundler program, but in some cases the bundler program will not function if the adware is removed, or will not install unless the adware is installed. Most Adware Bundlers install several adware applications from multiple adware vendors, each of which is governed by a separate End User License Agreement (EULA) and Privacy Policy. Some Adware Bundlers may not fully and properly disclose the presence of bundled advertising software during installation.

Adware, Low Risk

Low Risk Adware is advertising software that displays ads on the desktop but is installed with better notice, disclosure and user consent than the majority of adware programs. Nonetheless, some Low Risk Adware programs may still not fully disclose all potentially objectionable functionality during installation. Some Low Risk Adware programs display less intrusive forms of advertising, such as banner ads or text links embedded within the program itself. Low Risk Adware typically does not transmit personally identifiable information and is not considered a serious privacy risk.

Application

See program.

Anti-spyware Software

Software that protects a computer from spyware infection. Spyware protection software finds and removes spyware without system interruption.

Backdoor

A backdoor is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

Bot

See Zombie.

Botnet

Botnet is a collection of software robots (bots) that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software.

While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (zombies) running software, usually installed via worms, Trojans, or backdoors under a common command-and-control infrastructure.

Browser Hijacker or Overview Page Hijacker

A program that can change the settings in your Internet browser. Most often, this includes your search page URLs, in order to redirect all Internet searches to a specified pay-per-search site. Also targeted are your default home page settings, which can be diverted to another page, often a pornography site.

Browser Plug-in

A Browser Plug-in is a software module that is attached to the browser, usually Internet Explorer, and that works within the browser to provide additional functionality. Browser Plug-ins may be installed with adware and used to display advertising as well as redirect the browser to alternate sites and alternate search results. Many Browser Plug-ins also monitor user Web surfing and search data to facilitate targeted, contextual advertising. A toolbar is one type of Browser Plug-in.

Cookies

Cookies are small text files that websites place on your computer to recognize users. On subsequent visits to the same site, the cookie records information about your activity on it. This is often used to gauge where on a site individual users tend to frequent in order to develop page content tailored to each user's preferences and to improve offerings on the site so that you will come back to visit again.

While cookies are not harmful to your computer, they can be an issue of privacy. Tracking cookies are greatest risk to your privacy. They track your location on the Web - any site you visit.

Definitions

Definitions (often called threat definitions) are the basis that a antivirus or anti-spyware tool uses to compare against when protecting you from all sorts of malware, whether by scans, email protection, or real time protection.

Dialer (General)

A Dialer is a program that uses the computer's modem to dial telephone numbers, often without the user's knowledge and consent. A Dialer can connect to a toll number that adds long distance charges to the telephone bill without the user's knowledge or permission. Dialers may be downloaded through exploits and installed without notice and consent. A Dialer may be legitimate if downloaded and installed with full, meaningful, and informed user consent.

Drive-by download

When programs are downloaded without your knowledge or consent. This is most often accomplished when the user clicks to close or respond to a random advertisement or dialog box.

Exploit

An Exploit is software or code that targets security vulnerabilities, usually in the operating system or browser, but may also target vulnerabilities in other programs. Exploits are typically used to install malicious software on the victim's computer without the victim's knowledge or consent. An Exploit may be used to install malware that gives the attacker complete access to and control of the affected computer from a remote location.

Firewall

A firewall is an electronic barrier on your computer where that all information coming in and going out must travel. A firewall prevents external computer systems from communicating directly with your computer. A firewall analyzes information passing between the two computers, and rejects it if it does not conform to pre-configured rules (or exceptions).

High Risks

High risks are typically installed without user interaction through security exploits, and can severely compromise system security. Such risks may open illicit network connections, use polymorphic tactics to self-mutate, disable security software, modify system files, and install additional malware. These risks may also collect and transmit personally identifiable information (PII) without your consent and severely degrade the performance and stability of your computer.

Hijacker

Hijackers are software programs that modify users' default browser home page, search settings, error page settings, or desktop wallpaper without adequate notice, disclosure, or user consent. When the default home page is hijacked, the browser opens to the Web page set by the hijacker instead of the user's designated home page. In some cases, the hijacker may block users from restoring their desired home page. A search hijacker redirects search results to other pages and may transmit search and browsing data to unknown servers. An error page hijacker directs the browser to another page, usually an advertising page, instead of the usual error page when the requested URL is not found. A desktop hijacker replaces the desktop wallpaper with advertising for products and services on the desktop.

IRC bots

IRC (Internet Relay Chat) bots are sets of scripts or an independent program that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. It differs from a regular client in that instead of providing interactive access to IRC for a human user, it performs automated functions.

Joke Program

A Joke Program is software that is designed to mimic the actions of a virus but is not malicious and does not harm the machine.

Key Logger

A key logger is a program that captures and logs keystrokes on the computer without the user's knowledge and consent. The logged data may be encrypted and is typically sent to a remote attacker. The key logger is usually hidden from the user and may use cloaking (rootkit) technology to hide from other software in order to evade detection by anti-malware applications. Key loggers may be installed by trojans with other malicious software through exploits, and are often used by online criminal gangs to facilitate identity theft and bank fraud operations.

Known Risks (also known bads, known threats, or knowns)

A risk is described as being "known" based on GFI Software's definitions in the security risk database and has been determined as being harmful based on analysis and history of reported cases. Much of this information comes from users like you who have ThreatNet enabled. You may, however, consider a "known" to NOT be a risk to you (i.e. Hotbar). Some programs use adware that *you* may want to run on your computer. In this case, you will want to always allow it to run.

Low Risk

Low Risk programs/software should not harm your machine or compromise your privacy and security unless it has been installed without your knowledge and consent. A Low Risk Software application may be a program that you knowingly and deliberately installed and that you wish to keep. Although some Low Risk Software programs may track online habits—as provided for in a privacy policy or End User License Agreement (EULA)—or display advertising within the applications themselves, these programs have only vague, minimal, or negligible effects on your privacy.

Malware

Malware, short for malicious software, is a general term with clearly hostile or harmful functionality or behavior that is used to compromise and endanger individual PCs as well as entire networks.

Operating System

The operating system is the underlying software that enables you to interact with your computer. The operating system controls the computer's storage, communications, and task management functions. Examples of common operating systems include Microsoft Windows, MS-DOS, MacOS, and Linux.

Opt-out

Options presented by spam email. These options are often fake. For example, if you respond to a request to remove something, you may well be subjecting yourself to more spam. By responding, the sender knows that your email account is active. A 2002 study performed by the FTC demonstrated that in 63% of the cases where spam offered a "remove me" option, the option either did nothing or resulted in more spam email.

Phishing

Phishing is an email or instant messaging fraud method in which a message is sent to a recipient falsely claiming to be an established legitimate enterprise in an attempt to scam the recipient into surrendering private information that will be used for identity theft.

Typically, the messages appear to come from well-known and trustworthy websites, including PayPal, eBay, MSN, Yahoo, to name only a few. The message directs the recipient to visit a website where they are asked to update personal information, such as passwords, credit card, social security, and bank account numbers, that the legitimate organization already has. The website, however, is fraudulent and is set up only to steal the recipient’s information.

Defending against phishing:

Your best defense against phishing is your own diligence. Be cautious of any one or any message asking you to give out personal information, no matter how "legitimate" they appear on first glance. Verify they are who they say they are and be aware of their company's policy on asking for personal information.

To further protect you, VIPRE's anti-phishing feature in the Email Protection settings is designed to block anti-phishing messages from ever reaching your email Inbox.

POP3

Post Office Protocol (POP) is an application layer Internet standard protocol used by email programs to retrieve email from a remote server over a TCP/IP connection. POP3 servers use port 110. POP3 configuration is typically done from an email client.

Port

The most essential information in TCP and UDP packet is the source and destination port. The IP address identifies a computer in the Internet, whereas a port identifies an application running on the computer. Ports 1-1023 are reserved for standard services and the operating system, whereas ports 1024-65535 can be used by any application. In a typical client to server connection, usually the destination port is known (connection is established for this port or UDP datagram is sent to it). The source port is then assigned by the operating system automatically.

P2P Program

A P2P (or Peer to Peer) Program is software that enables the user to participate in an online file sharing network and trade or share files with other users in the network. P2P Programs often bundle advertising software, but some P2P Programs are adware-free. P2P Programs are typically not harmful in and of themselves, but the user is at risk for infection with adware and/or malware though files downloaded from the file sharing network.

Program

A program or application is a set of instructions directing the computer to perform a task. This could be anything, from adding two numbers and outputting the result, to the complex instructions in the program of a computer game. A program can be safe or harmful.

Risk

See Known Risks.

Risk Definitions

See definitions.

Rogue Security Program

A rogue security program is software of unknown or questionable origin. Rogue security programs usually show up on websites or SPAM emails as intrusive warnings that claim that your computer is infected and offer to scan and clean it. These should never be trusted. Reputable antivirus or anti-spyware companies will NEVER use this way of "notifying" you. A rogue security program may appear like an ordinary antivirus or anti-malware program, but will instead attempt to dupe or badger you into purchasing the program. While some rogue security programs no good, others may result in harm by installing malware or even stealing the credit information that you enter, possibly resulting in identity theft.

Rootkit

A rootkit is software that cloaks the presence of files and data to evade detection, while allowing an attacker to take control of the machine without the user's knowledge. Rootkits are typically used by malware including viruses, spyware, trojans, and backdoors, to conceal themselves from the user and malware detection software such as antivirus and anti-spyware applications. Rootkits are also used by some adware applications and DRM

(Digital Rights Management) programs to thwart the removal of that unwanted software by users.

Service (Windows Service)

A Service is an executable that performs specific functions and is designed not to require user intervention. A service usually starts when the Windows operating system is booted and runs in the background as long as Windows is running. If the VIPRE service fails, you can manually start the service.

Shareware

Software that is distributed for evaluation without cost. Shareware usually requires payment to the author for full rights to the software.

Spam

Unsolicited commercial email. It is often sent in bulk, via "open-relays" to millions of computer email accounts. It takes a toll on an Internet users' time, their computer resources, and the resources of Internet Service Providers (ISP). Most recently, spammers have begun to send advertisements via text message to cell phones.

Spyware

Spyware is software that transmits information to a third party without notifying you. It is also referred to as trackware, hijackware, scumware, snoopware, and thiefware. Some privacy advocates even call legitimate access control, filtering, Internet monitoring, password recovery, security, and surveillance software "spyware" because those could be used without notifying you.

Surveillance

A Surveillance Tool is a program that monitors and captures data from a computer including screenshots, keystrokes, Web cam and microphone data, instant messaging, email, websites visited, programs run and files accessed and files shared on a P2P (peer to peer) network. Many Surveillance Tools can run in stealth mode, hidden from the user, and have the ability to store captured data for later retrieval by or transmission to another computer.

System Snooper

A System Snooper is a program that is used to monitor and record data on the computer's usage. System Snoopers may track address bar URLs, browser cache, search history, file download history, recently used documents, recently run programs, cookies, and index.dat files. While System Snoopers may have legitimate uses, they may also be used to monitor other people's computer use without their knowledge and consent. Some System Snoopers are easily visible to the user, while others may be hidden.

Threat

See Known Risks.

Threat Definitions

See definitions.

Toolbar

A Toolbar is a type of browser plug-in that adds a third-party utility bar to the Web browser, usually just below or next to the browser's address bar. A Toolbar typically has a search function and provides search results for paid advertisers. It often has buttons that are links to advertisers' Web pages. An advertising toolbar may track browsing and search queries in order to display contextually relevant search results and ads.

Traces

A trace is the smallest unit of malware that is detected and can include files, folders, or Registry keys/values. A risk is made up of these smaller units.

Trojan

A trojan is installed under false or deceptive pretenses and often without the user's full knowledge and consent. In other words, what may appear to be completely harmless to a user is in fact harmful by containing malicious code. Most trojans exhibit some form of malicious, hostile, or harmful functionality or behavior.

Unauthorized Program

An Unauthorized Program in an I.T. environment could be any software program installed by users on the network that is not compliant with the I.T. and security policies of the network owner or administrator.

Unknown

A potential risk that has yet to be established as a "known" risk by GFI Software's security risk database. An unknown could be safe to *your* computer; it just has yet to be determined to be either safe or unsafe.

Virus

A computer virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as CD-ROMs or flash drives. Viruses can also spread via email through infected attachments and files. Most viruses include a "payload" that can be anywhere from annoying and disruptive to harmful and damaging; viruses can cause system damage, loss of valuable data, or can be used to install other malware.

Worm

A worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike viruses, however, worms spread without attaching to or infecting other programs and files. A worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through email by sending copies of itself to everyone in the user's address book. A worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some worms may be used to compromise infected machines and download additional malicious software.

Zombie/Bot

Zombies and Bots are programs used to compromise a computer and allow it to be remotely exploited by an attacker for specific malicious tasks. A computer infected with a Zombie or Bot may be used by an attacker to send spam, participate in a Distributed Denial of Service (DDOS) attack against websites or other computers, or install adware and spyware for monetary gain. The "zombied" or compromised computer becomes part of a Botnet—a large network of other compromised machines that are controlled and used for malicious purposes by the Bot master.

7 Appendix II: Troubleshooting

Troubleshooting: Computer Performance Issues

Are you running another antivirus or anti-spyware product?

Running more than one antivirus, anti-spyware, or anti-malware product (e.g. AVG, Kaspersky, McAfee, Norton, NOD32, Panda, Symantec, ZoneAlarm, etc.) with real-time protection turned on can affect your computer's performance. Only one should be active at a time. In addition, you can use several scan tools to perform manual scans, but do so one at a time for the best performance. Please refer to those products' documentation for specific advice.

Is VIPRE currently scanning?

If VIPRE is scanning and you are running other programs that require large amounts of memory, such as computer games and video/image editing, you may want to consider discontinuing the scan and running it later. You can do any of the following:

- To temporarily pause the scan, right-click on the green VIPRE icon in your system tray (lower-right corner of your computer screen) and select **Scan>Pause Scan**. You can resume the scan later by selecting **Scan>Resume Scan**.
- To cancel the scan, right-click on the green VIPRE icon in your system tray (lower-right corner of your computer screen) and select **Scan>Abort Scan**. You can run the scan again later by selecting **Scan>Quick** or **Deep**.

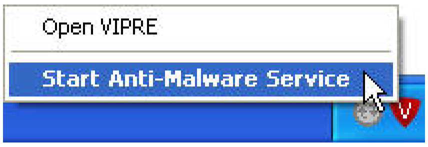
> **Tip:** Schedule a scan to run during a time that your computer is most likely not being used and will be turned on. How?

Troubleshooting: VIPRE Icon in the System Tray is Red

If the VIPRE icon in your system tray (lower-right area of your computer screen) is red , you are being alerted that the VIPRE service is disabled. You will need to restart the service.

To start the VIPRE service:

1. Right-click on the red VIPRE icon and then select **Start Anti-Malware Service** from the menu.

   The VIPRE service starts and should be running normally. Also, the icon will change from red to blue or gray .
2. Please, contact Technical Support if you are still experiencing problems.

Switching to Safe-Mode

There may be times when your computer is infected so badly that you need to run a deep scan from Safe Mode. Safe Mode with Networking only loads the very basic files needed to run Windows, giving the antivirus programs a better chance of removing all the files associated with the threat(s).

If Windows XP, Vista, or Win7 is the only operating system installed on your computer, boot into Safe Mode with Networking by following the instructions listed below:

To run your computer in Safe Mode:

1. If the computer is running, shut down your computer.
2. Wait 30 seconds, and then turn the computer’s power back on.
3. Start continuously tapping the **F8** key until the Windows Advanced Options Menu appears.

    Note: If you begin tapping the F8 key too soon, some computers display a "keyboard error" message. To resolve this, go back to Step 1 and try again.

4. Ensure that the **Safe Mode with Networking** option is highlighted, and then press **Enter**. The computer will then begin to start in Safe Mode with Networking.

8 Contacting GFI Software

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

ENGLAND AND IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK
Telephone: +44 (0) 870 770 5370
Fax: +44 (0) 870 770 5377
sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta
Telephone: +356 2205 2000
Fax: +356 2138 2419
sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia
Telephone: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com